Office of the Information Commissioner
Queensland

16 December 2020

Level 7
133 Mary Street
Brisbane Q 4000

PO Box 10143
Adelaide Street
Brisbane Q 4000

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

ABN: 70 810 284 665

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

By electronic submission

Digital Identity Legislation Consultation Paper

The Queensland Office of the Information Commissioner (**OIC**) welcomes the opportunity to provide a submission in response to the Digital Identity Legislation Consultation Paper (**Consultation Paper**).

While OIC acknowledges 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, it can also raise significant privacy issues.

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.

OIC provides the following high-level comments in response to the Consultation Paper:

1. Development of Digital Identity without legislation in place to support the National Driver Licence Facial Recognition Solution

The re-introduced Commonwealth Identity-Matching Services Bill 2019 (**IMS Bill**) is yet to be passed. 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.

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.

In October 2019, the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) recommended[1] the IMS Bill be 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.

These principles include: the regime should be built around privacy, transparency and robust safeguards, the regime should be subject to Parliamentary oversight and reasonable, proportionate and transparent functionality and the regime should be one that requires reporting on the use of identity-matching services.[2] These broad principles are equally applicable to the development of a legislative framework to support Digital Identity.

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. 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. The timeframe for the IMS Bill to be passed and operational remains uncertain.

2. Express legislative requirement for a Privacy Impact Assessment (PIA)

OIC notes that currently, as part of the Trusted Digital Identity Framework (**TDIF**), entities seeking accreditation must submit a PIA for their product. Australian Government agencies must conduct PIAs for high privacy risk projects under the Australian Government Agencies Privacy Code. However, this is not an explicit requirement for private sector organisations covered by the Commonwealth Privacy Act (**Privacy Act**), or other organisations not covered by the Privacy Act.

OIC considers the requirement for a PIA should be expressly required by the Digital Identity Legislation. Further, the PIAs should be updated throughout the lifecycle of the project and, in the interests of transparency and accountability, made publicly available.[3] Release of the PIAs publicly, to the greatest extent appropriate, in conjunction with a comprehensive community education program about the Digital Identity is essential to build community trust and confidence in the Digital Identity program.

Community concerns over privacy and the government's ability to protect their personal information and secondary use of data, whether real or perceived risks, have the potential to undermine community trust and confidence resulting in reduced levels of take up by the community. The uptake of the My Health Record and more recently

[1] 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.
[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,* at page 76.
[3] noting that it may not always be appropriate to publish the full PIA.

the *COVIDSafe* app demonstrate the importance of social licence to the success of new initiatives and programs, such as Digital Identity.

3. Enshrine key privacy and data security protections in primary legislation

OIC notes the following proposed structure of the Legislative Framework:

- Primary legislation
- Operating rules and other legislative instruments
- The TDIF and other written policies.

OIC further notes that it is proposed that the TDIF will continue to set out the minimum requirements entities must meet to achieve and maintain TDIF accreditation. This spans security, privacy, accessibility, usability, service operations, fraud prevention measures and technical integration matters. As outlined in the Consultation Paper, while parts of the TDIF will be enshrined in law, the TDIF will not be a legislative instrument itself, but will remain a standalone and distinct policy.

As outlined in the Consultation Paper, the privacy provisions in the TDIF are designed to address specific concerns around the system relating to:

- possible commercialisation of data and profiling of Users
- the development of a single national identifier or a national surveillance database
- gradual or incremental changes to the system that might result in an erosion of privacy over time
- the use of Biometric Information without clear protections

It has been OIC's consistent position that data and privacy protections and safeguards for Digital Identity, such as those provided for by TDIF, should be the subject of explicit provisions enshrined in primary legislation rather than in other mechanisms such as legislative instruments and written policies. This provides for a level of parliamentary oversight and scrutiny of any proposed amendments that may serve to weaken privacy protections that is not available for protections prescribed in other legislative instruments or written policies.

The recent passing of the *Privacy Amendment (Public Health Contact Information) Act 2020* by the Commonwealth Government demonstrates the extent and nature of privacy protections required to be entrenched in primary legislation, including mandatory reporting of data breaches, to gain the trust of the community to facilitate the uptake of the *COVIDSafe* app.

These learnings are relevant to the extent of data security and privacy protections and safeguards required to be entrenched in the Digital Identity Legislation. At a high level, this will include (noting this is not an exhaustive list):

- express limits on the use of digital identity information for clearly defined prescribed purposes
- ensuring the system remains entirely voluntary and reflects contemporary developments in privacy law regarding the meaning of 'consent'
- prohibition on the commercialisation of personal information and profiling of individuals
- restrictions on the creation and use of a single identifier for the whole system

- penalties and/or other sanctions, including criminal sanctions, for use of digital identity information other than for prescribed purposes
- protection against coercing individuals to obtain a digital identity and recognition that cohorts such as remote indigenous communities could face digital exclusion unless adequately accommodated
- mandatory data breach notification scheme and system for managing complaints
- mandated regular transparent reporting requirements on the operation of the Digital Identity program
- robust independent oversight of the Digital Identity Program including regular auditing of use and access, including data security assessments
- timeframe for deletion of data in the event an individual no longer wishes to retain a digital identity
- retention of digital identity data on databases inside Australia; and
- robust data security safeguards being adequately funded to prevent unauthorised access and loss of identity credentials.

4. Consistency of privacy laws across jurisdictions – implications for state and territory participation

As noted in the Consultation Paper, it is intended for states and territories with privacy legislation, that the legislation will allow state and territory entities to participate in the system as Accredited Participants where their legislation offer equivalent levels of privacy protection to the Privacy Act. OIC notes that an approach to determining equivalence will be the subject of further consultation with local and national regulators. The Consultation paper proposes that for state and territory entities participating in the system as Accredited Participants in jurisdictions without equivalent privacy legislation, it is proposed to treat these entities as organisations under the Privacy Act, binding these entities to the Australian Privacy Principles and other provisions of the Privacy Act.

Inconsistencies in privacy legislation across Commonwealth, State and Territory jurisdictions, leads to gaps in privacy protections afforded to individuals, including limiting opportunities for individuals to seek recourse in the event of a data breach. OIC notes that there is currently an absence of existing privacy legislation in South Australian and Western Australia. Sharing of personal information between jurisdictions is problematic where there is variance between, or absence of, legislated privacy safeguards across jurisdictions.

This issue was considered by the Committee in their report on the IMS Bill. The Committee recommended that all users of the identity-matching services should be subject to a law or legally enforceable agreement that protects personal information in accordance with the Australian Privacy Principles and as a matter of principle, the IMS Bill should not enable personal information held by an agency in a jurisdiction with strong, legislated privacy safeguards to be shared with an agency in another jurisdiction where such safeguards may not exist. The Committee noted that some State and

Territory jurisdictions may have to enact new privacy legislation in order to satisfy such a requirement.[4]

OIC provides in-principle support for alignment with privacy protections afforded by the Australian Privacy Principles to underpin participation by jurisdictions, including Queensland, in a national federated Digital Identity program and inclusion of a similar express requirement in the Digital Identity legislation. However, OIC has previously raised that it is not certain that Queensland's current privacy laws offer equivalent coverage to the Privacy Act. The current review of the Privacy Act may lead to greater alignment with the European General Data Protection Regulation (GDPR), further widening the gap between Commonwealth, State and Territory privacy legislation. This has implications for Queensland's existing privacy legislation and participation by this jurisdiction in a national federated Digital Identity program.

Recommendations have been made to strengthen and update Queensland's privacy legislation, including the reforms recently discussed and recommended by the Crime and Corruption Commission (**CCC**) in their report into misuse of confidential information in the Queensland public sector, including introduction of a mandatory data breach notification scheme. The legislative amendments to the *Information Privacy Act 2009* (Qld) (**IP Act**) recommended in the CCC's report are largely consistent with the recommendations made by OIC to the 2016 Consultation on the review of the *Right to Information Act 2009* and the IP Act. Implementation of the recommendations is subject to Queensland Government response and implementation. This is a matter for the Queensland Attorney-General and Minister for Justice.

Without such legislative change, exploration of options for Queensland to opt-in to coverage and protections afforded by the Privacy Act would require further careful consideration, including obtaining advice about the legal or any other ramifications this may have for this jurisdiction.

Yours sincerely

Rachael Rangihaeata
Information Commissioner

Phil Green
Privacy Commissioner

[4] 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*, at page 79.