information and privacy commission
new south wales

[redacted]
**Our reference: IPC21/A000277**

7 July 2021

Digital Transformation Agency
PO Box 457
Canberra City ACT 2601

By email: digitalidentity@dta.gov.au

Dear Sir/Madam

**DIGITAL IDENTITY LEGISLATION POSITION PAPER**

This is a submission to the Digital Identity Legislation Position Paper released by the Australian Government's Digital Transformation Agency. This submission provides general comments and specific responses to identified policy proposals outlined in the position paper.

The NSW Privacy Commissioner administers the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act) and promotes awareness and understanding of privacy rights in NSW. The PPIP Act and HRIP Act establish the Information Protection Principles and Health Privacy Principles which govern the collection, security, use and disclosure of personal and health information by NSW government agencies and, in the case of the HRIP Act, private sector health care providers.

**Privacy Safeguards**

As NSW Privacy Commissioner I support the inclusion of specific privacy safeguards in the primary legislation. This will assist in building user trust in the digital identity system and provide individuals with clear knowledge concerning how their personal information will be used, who can access their personal information and for what purposes, and penalties for misuse of personal information.

In particular I am pleased to note the following features of the legislation as detailed in the position paper:

- the definition of Digital Identity information will include a non-exhaustive list of examples, with further details to be set out in the rules
- requiring individuals to expressly consent before their attributes are shared with a relying party
- requiring relying parties to provide an alternative channel to digital identity for individuals to access their services (subject to some exemptions)
- prohibiting the creation of a single identifier used across the system and all government services
- restrictions on the use of digital identify information for direct marketing or profiling and

- restrictions on the use of biometric information, including limiting the system to one-to-one biometric matching only, preventing biometric information being sent to third parties, requiring biometric information to be deleted once it has been used for its intended purpose, and requiring users consent before their biometric information can be accessed for fraud or security investigations.

The additional proposals outlined in the position paper will positively enhance the privacy protections built into the identity system and are supported, in particular the proposals at:

- paragraph 7.4.14 that state and territory government entities that are Accredited Participants and are not covered by the *Privacy Act 1988* (Cth) (Privacy Act), will have the option of complying with a comparable state or territory privacy law
- paragraph 7.4.7 that the rules will require applicants for TDIF accreditation to commission an independent assessor to conduct a Privacy Impact Assessment (PIA) as a requirement of their accreditation
- paragraph 7.4.9 that the rules will contain a specific prohibition on identity exchanges from retaining any User attributes once they are passed from an identity provider to a relying party
- paragraph 7.4.10 that the rules will require identity exchanges on the Participant Register to provide Users with a centralised view of their metadata, specifically, the relying party's services the User has accessed; the date and time of access; and the categories or types of attributes passed to the relying party.

**Exemptions**

The position paper proposes that the legislation will require a relying party to provide an alternative channel to Digital Identity to enable individuals to access its services provided the relying party's service is not an essential service or is the only provider of that service unless granted an exemption by the Oversight Authority. The legislation should include a clear definition of "essential service".

**Data breaches**

For state and territory government bodies that are Accredited Participants but not subject to the Privacy Act or a comparable notifiable data breach (NDB) scheme, it is proposed at paragraph 7.4.15, that if the body has reasonable grounds to believe that a NDB has occurred, the body will be required to provide a statement about the breach to the Oversight Authority. The body will also need to notify affected individuals in a similar manner to the NDB scheme.

It should be noted that NSW is currently developing a model for a mandatory data breach notification scheme and it is anticipated that this scheme will be legislated in 2021. Upon commencement of the scheme, NSW public sector agencies will be required to notify the NSW Privacy Commissioner of eligible data breaches, as well as notify affected individuals.

Consideration will need to be given to notification and investigation arrangements in circumstances where a breach involves multiple organisations subject to different privacy law regimes.

Given the potential for breaches to involve overlapping jurisdictions, I would expect to see provisions in either the primary or subordinate legislation concerning referrals between the Office of the Australian Information Commissioner (OAIC) and the equivalent state or territory regulators. I note the proposal at paragraph 7.4.15 information sharing arrangements between the OAIC and state or territory regulators to facilitate investigations.

**Governance arrangements**

*Independence of the Oversight Authority*

The position paper proposes the establishment of an Oversight Authority led by an independent statutory officer. I note, however, that no provision has been made for the establishment of a separate independent office to support the statutory officer to fulfill their functions. Instead the paper anticipates that the Oversight Authority will be located within an existing government department or agency.

As a regulator, it is important that the statutory officer is supported by a separate office and has full control of their budget and staff. This will increase public confidence in the independence of the Oversight Authority and will reduce the potential for conflicts of interest to arise that may impede the statutory officer's ability to fulfil their functions. The establishment of a separate independent office to support the statutory officer would be a preferable approach.

*Functions of the Australian Information Commissioner*

Additionally, the position paper proposes the Australian Information Commissioner would be responsible for privacy functions under the scheme that relate to the privacy of an individual, authorised by section 9 of the *Australian Information Commissioner Act 2010* (the AIC Act). As part of this proposal, the Information Commissioner would report on the Digital Identity privacy function in the annual report required under the Privacy Act. While this proposal would contribute to strengthening governance arrangements for the Digital Identity system, it is crucial that any allocation of additional functions to the Information Commissioner is accompanied by commensurate levels of additional resourcing.

**Liability Framework**

I am pleased to observe that the position paper now proposes that the legislation contain a mechanism to provide redress for users exposed to identity theft or loss due to cyber security incidents.

I hope that these comments will be of assistance in your consideration of this matter. Please do not hesitate to contact me if you have any queries. Alternatively, you may contact [redacted] or by email at [redacted].

Yours sincerely

[redacted]

Samantha Gavel
**Privacy Commissioner**