



information
and privacy
commission
new south wales

Enquiries: ipcinfo@ipc.nsw.gov.au
Telephone: 1800 472 679
Our reference: IPC23/A000314

10 October 2023

Department of Finance
1 Canberra Avenue
Canberra ACT 2603

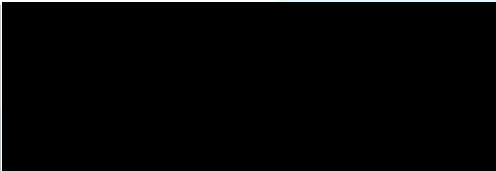
Dear Sir/Madam

COMMONWEALTH DIGITAL ID LEGISLATION CONSULTATION

I welcome the opportunity to make a submission to the Department of Finance on the Digital ID Legislation Consultation.

Enclosed below is the submission from the Information and Privacy Commission NSW (IPC).

Please do not hesitate to contact the IPC if you require any further information. Alternatively, your officers can contact Darby Judd, Senior Policy Officer on 1800 472 679 or via ipcinfo@ipc.nsw.gov.au.



A/Privacy Commissioner

Encl.



information
and privacy
commission
new south wales

Commonwealth Digital ID Legislation Consultation

Submission by the Information and Privacy Commission NSW


10 October 2023

Sonia Minutillo

A/Privacy Commissioner

The Commissioner's signature has not been included in this submission to facilitate public access to the submission, manage security risks and promote availability in accordance with the *Redacting signatures on public facing documents Practice Guide* published on the IPC website.

The Information and Privacy Commission NSW (IPC) welcomes the opportunity to provide a submission to the Commonwealth Digital ID Legislation Consultation.

 The Information and Privacy Commission NSW (IPC) oversees the operation of privacy and information law in New South Wales.

The Privacy Commissioner has responsibility for overseeing and advising NSW public sector agencies on compliance with the *Privacy and Personal Information Protection Act 1998* (PPIP Act) and the *Health Records and Information Privacy Act 2002* (HRIP Act).

The IPC is an integrity agency with functions that are fundamental to the preservation and advancement of representative democratic Government. Section 3 of the GIPA Act provides that the object of the legislation is to open government information to the public in order to maintain and advance a system of responsible and representative democratic Government that is open, accountable, fair and effective.

For further information about the IPC visit www.ipc.nsw.gov.au.

IPC Response: Key questions on the Digital ID legislation and Digital ID Rules

General Comment: Risks from non-accredited entities under a voluntary scheme

The Digital ID legislation establishes a voluntary Digital ID accreditation scheme. I note the practical constraints in making the scheme mandatory. Nonetheless, the voluntary nature of an accreditation scheme, in which non-accredited private sector entities would be eligible to request that customers share their Digital IDs to validate customers identities when accessing certain services, remains a concern from a privacy perspective. Any voluntary scheme should be underpinned by strong community education and effective public messaging to ensure that consumers are aware of their own personal risks that they will assume in transacting with non-accredited providers and the benefits and associated safeguards that will be derived from an accredited scheme.

The remaining comments below relate to the Privacy Safeguards as they apply to entities that do fall under the accreditation scheme.

Privacy Safeguards

Question: Are the additional privacy safeguards sufficiently robust, clear and practical?

I note that the Digital ID Bill 2023 (the Bill) provides specific protections tailored to the Digital ID context which are additional and build upon the existing privacy safeguards. Notwithstanding this, the Bill does not duplicate existing regulatory frameworks. In particular, I note that accredited entities will be subject to whichever notifiable data breach scheme is in place under either the *Privacy Act 1988* (Cth) (the Privacy Act) or the equivalent state/territory data breach scheme. In the case of NSW, this would mean accredited entities would be subject to the Mandatory Notification of Data Breach (MNDB) Scheme under the PPIP Act. I also note that to the extent an entity is not covered by a notifiable data breach scheme, the Bill's provisions extend the Privacy Act's scheme to that entity. In my view, this is a welcome and sensible provision of the Bill.

The additional privacy safeguards that the Bill will introduce, which will be regulated by the Information Commissioner (Cth), and that all accredited entities will be subject to, will positively enhance the privacy protections built into the Digital ID system and are supported by the IPC. In particular, the IPC supports the following:

- The protection to prohibit the intentional collection of certain 'attributes' (attributes taken to mean a person's racial or ethnic origin, political opinions, religious beliefs, or sexual orientation).
- The requirement for accredited entities to obtain the user's express consent before sharing user information.
- The protection against the disclosure of an individual's restricted attributes (e.g. passport or licence number) unless authorised by an accreditation condition or an individual's express consent.
- The protection against the disclosure of an individual's unique identifier to ensure it cannot be used to track a person's online behaviour or the services they access (with exemptions if the disclosure is necessary to detect fraud).
- A range of safeguards on the use of biometric information by accredited entities, including:
 - The prohibition from a person's biometric information being used by an accredited entity to compare against biometric information to identify the individual.
 - The collection and use of biometric information for verification and authentication purposes only.
 - Retaining of biometrics information only where an individual has consented.

- Limited secondary uses of biometrics information only for the purposes of fraud investigation and testing, disclosure to the individual involved, and disclosure to law enforcement with a warrant issued by a magistrate, judge or tribunal, or consent for an investigation/prosecution or identity verification.
- Rules to govern emerging issues involving biometric information, in particular, the allowance for the Minister to make rules, disallowable by Parliament, to allow disclosure of biometric information where the disclosure is to allow an individual in control of their own verifiable credential to expressly consent to share that credential.
- Prohibiting accredited entities from using or disclosing information about an individual's online activities except in permitted circumstances.
- Prohibiting accredited entities from using or disclosing an individual's personal information for marketing purposes that are unrelated to the Digital ID services the entity provides to the individual.
- The requirement for accredited identity exchange's to not retain an individual's name, address, date of birth, phone number, email, or restricted attributes.

It is my view that the above safeguards, as they apply to accredited entities, are sufficiently robust, clear, and practical. The safeguards provide a sound framework to protect citizens' personal information from improper use and disclosure, which is consistent with existing NSW Privacy laws. This will allow for the use and disclosure of information where it is technically necessary and practicable, and where consent has been provided, or for the purposes of specific activities related to law enforcement.

Question: Is the rule making power to allow disclosure of biometric information to enable sharing of verifiable credentials (under specified circumstances) an appropriate exception to the restriction on disclosure of biometric information?

The Bill places a range of restrictions on the use and disclosure of biometric information by accredited entities, including:

- Biometrics can only be retained for verification and authentication purposes and must be deleted after that use ceases.
- In relation to authentication, biometrics can be retained where the individual has consented so the biometric can be used to authenticate the individual in the future. The rules may require that biometrics are stored in an encrypted manner or on the individual's local device to prevent access to the original image while maintaining the authentication functionality.
- Only limited secondary uses of biometrics, including:
 - for fraud investigation and testing.
 - disclosure to the individual involved.
 - disclosure to law enforcement with a warrant issued by a magistrate, judge or tribunal.
 - disclosure to law enforcement with consent for an investigation/prosecution or identity verification.

I note that the restrictions on the disclosure of biometric information are sound in most circumstances. However, in some circumstances, they may affect an individual's ability to use verifiable credentials if they become part of the Accreditation Scheme in the future. To allow the sharing of verifiable credentials in these circumstances, the Bill will allow for the Minister to make rules, disallowable by Parliament, to facilitate the disclosure of biometric information where the disclosure is to allow an individual in control of their own verifiable credential to expressly consent to share that credential. Additionally, the Minister must consult with the Information Commissioner (Cth) before making any rules about biometrics.

In circumstances where an individual expressly consents to their biometric information to be shared, in order to verify a credential, such as a rule-making power to allow the disclosure of biometric information. It is in my view that this is an appropriate exemption, as it is consistent with the protection in the Bill, which requires the individual to give their consent to the use or disclosure of their biometric information or verifiable credential. Furthermore, the provision mandating that the Minister consult with the Information Commissioner (Cth), as the administrator of the Privacy Act, as the regulator and enforcer of these additional safeguards, is also consistent with the principles of good governance, transparency, and accountability.

Question: Is the maximum penalty for a breach of a privacy safeguard sufficient to deter accredited entities from interfering with a person's privacy? If not, what maximum penalty would be an appropriate deterrent?

The provisions within the Bill are written to indicate that the penalties are to apply to accredited entities, but it is unclear as to whether they may also apply to individuals within the organisation. I note that under the Commonwealth's Notifiable Data Breaches Scheme, that the penalties for a serious or substantial breaches, whichever is the greater of, are as follows:

- \$50 million
- three times the value of any benefit obtained through the misuse of information, or
- 30% of a company's adjusted turnover in the relevant period.

For individuals, the maximum penalty is \$2.5 million.

Given that the proposed legislation is set to function alongside the existing Privacy Act and Notifiable Data Breaches Scheme, I am of the understanding that all entities transacting with Digital IDs would continue to be subject to these penalties in the event of a serious or substantial data breach, in addition to the maximum penalties proposed under the new Bill.

In circumstances where the Commonwealth Notifiable Data Breaches Scheme provides individual penalties, the Bill may wish to address the scope of the penalties as they relate to individuals within these organisations who might be responsible for breaching, and or making decisions, which lead to the breach of privacy safeguards.

Accreditation Process

Question: Is the application for accreditation process appropriate, or should other matters be included, or some excluded?

Finally, I note that in order to gain accreditation, accredited entities must comply with strict accreditation conditions specified in the Act, the Accreditation Rules and any special conditions imposed by the Regulator. I note that, in particular, the requirement for applicants to submit a Privacy Impact Assessment (PIA) which must be conducted according to 2.3 of the Digital ID Accreditation Rules 2024, which extensively details the requirements of the PIA to ensure the protection of privacy, including but not limited to which includes but is not limited to, the privacy impact and risks to the applicant's Digital ID data environment and accredited services. Additionally, the PIA must assess the entity's compliance against the Privacy Safeguards detailed in Chapter 3 of the Bill as detailed in the section above (Privacy Safeguards), as well as compliance with the privacy rules in Chapter 4, Part 3 of the Rules which specifies the requirement for applicants to comply with the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth) including the need for entities to undertake the following:

- Develop privacy policies and adequate process to regularly review the policies.
- Adherence to data minimisation principles.
- Disclose fraud activities.
- Privacy awareness training.
- Develop a data breach response plan.

- Practice sound record keeping.

These requirements for accreditation are extensive and follow similar best practice principles and standards to which NSW Government agencies are held to under the PPIP Act, and as such I see the accreditation process as appropriate as it is outlined in the accreditation rules.

I also note that to date, there have been four independent PIAs conducted on the Australian Government's Digital ID system and associated policy, which include the following:

- Privacy Impact Assessment Report for the draft TDI Legislation, February 2022, HWL Ebsworth
- 3rd Independent Privacy Impact Assessment (PIA) on the TDIF and related Digital Identity Eco-system, March 2021, Galexia
- Second Independent Privacy Impact Assessment (PIA) for the Trusted Digital Identity Framework (TDIF), September 2018, Galexia
- Initial Privacy Impact Assessment (PIA) for the Trusted Digital Identity Framework (TDIF) Alpha, December 2016, Galexia

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 Darby Judd, Senior Policy Officer, by email at darby.judd@ipc.nsw.gov.au.

Yours sincerely

Sonia Minutillo
A/Privacy Commissioner