Australian Government

Office of the Australian Information Commissioner

Digital Identity Legislation Consultation Paper - Submission to the Digital Transformation Agency

Elizabeth Hampton

Acting Australian Information Commissioner and Privacy Commissioner

18 December 2020

OAIC

Contents

1. Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Digital Transformation Agency's (DTA) Digital Identity Legislation Consultation Paper (Paper). The Paper seeks views on proposed legislation that will support an expanded Digital Identity system (system) in Australia.

2. More specifically, the proposed Digital Identity legislation (legislation) intends to:

   - embed the privacy protections of the system in law, including safeguards currently contained in the Trusted Digital Identity Framework (TDIF)
   - support the Government's expansion of the system to a broader suite of non-Commonwealth entities, including the private sector and states and territories
   - formalise the appointment and the scope of powers for an Oversight Authority (or authorities).

3. The OAIC supports the Australian Government's ongoing development and proposed codification of the system, with the aim of providing individuals with a safe, simple and secure way to verify their identity online.

4. The OAIC has engaged with the DTA over a number of years on the development of the TDIF, reflecting the significant privacy implications of digital identity management. Most recently, we have participated as a member of the Digital Identity and MyGov Steering Committee, and as an observer on an Interdepartmental Committee to develop the legislation for the system. The OAIC welcomes the DTA's commitment to ensuring the system incorporates robust privacy safeguards and we support implementation of the 2018 Privacy Impact Assessment which recommended the important privacy protections in the TDIF be enshrined in legislation.

5. Given the system is proposed to rely on voluntary participation, ensuring robust privacy protections are incorporated into legislation is fundamental to its effectiveness. The legislative and policy framework must give Accredited Participants, relying parties and individuals the confidence to join a system that will facilitate online identity verification while protecting privacy.

6. The Australian community is highly attuned to the importance of protecting personal information. At the same time the community is reporting decreasing levels of trust in information handling by both business and government. The OAIC's Australian Community Attitudes to Privacy Survey (ACAPS) 2020[1] results reveal:

   - 85% have a clear understanding of why they should protect their personal information
   - 97% consider privacy important when choosing a digital service
   - since the 2007 ACAPS, trust in companies in general is down by 13% and trust in Federal Government departments is down 14%.

[1] OAIC (2020) *Australian Community Attitudes to Privacy Survey 2020*, report prepared by Lonergan Research.

7. These results have relevance to the development of the system, given both the nature of digital identity management and the proposed economy-wide expansion of the system.

8. This submission highlights the importance of independent oversight of regulatory settings, including clear lines accountability for the handling of personal information. This will assure individuals that the entities given authority to verify and use personal information must comply with a robust legislative framework that includes strong enforcement mechanisms. The OAIC considers that it is well positioned to function as the Oversight Authority for the privacy aspects of the system, given its expertise and independent regulatory remit.

2. Proposed legislative framework

Primary legislation

9. The legislative framework proposed to underpin the system would comprise:

- primary legislation
- Operating Rules and other legislative instruments
- the TDIF and other written policies.

10. The OAIC recommends that privacy protections are embedded in legislation. It is important to ensure that provisions governing the handling of personal information are subject to robust parliamentary and public scrutiny.

11. Secondary legislation affords flexibility to change procedural, subject matter specific obligations more easily, however primary legislation, rather than subordinate instruments, provides the strongest privacy protective measures. Legislative instruments such as the Operating Rules should support the legislation and operate as a mechanism through which to prescribe greater specificity in relation to the obligations.

12. Embedding privacy protections in primary legislation also guards against inadvertent or unforeseen risks to privacy, such as the collection, use or disclosure of personal information that may not have been originally intended, known as 'function creep', or that which may not be reasonable, necessary and proportionate to the relevant policy objectives.

13. The OAIC recommends that the legislation explicitly limit the collection, use and disclosure of personal information to the purposes of:

- verifying identity and providing assistance to receive digital services from a Relying Party
- supporting fraud management functions
- de-identifying data to create data sets for research purposes.

14. The OAIC recommends that the legislation incorporate restrictions on certain commercial activities, including direct marketing.

15. The following are examples of the privacy protections that would warrant inclusion in primary legislation:

- the voluntary nature of the creation and use of a digital identity
- provision of meaningful alternative identity verification channels
- prohibition on the creation of single, unique system-wide identifiers
- maintenance of a 'Digital Identity Participant Register' by the Oversight Authority
- data profiling limitations
- data retention periods
- prohibiting improper disclosure of sensitive or other personal information
- the obligation to undertake a Privacy Impact Assessment
- the handling of biometric information.

Recommendation 1 – Privacy protections should be contained in primary legislation, rather than subordinate instruments such as the Operating Rules.

Recommendation 2 - The legislation should explicitly limit the collection, use, and disclosure of personal information to specific purposes.

3. Proposed privacy protections

The application of the Privacy Act to participants in the system

16. The OAIC recognises that digital identity is a whole-of-economy initiative. The legislation must therefore provide a comprehensive and consistent legal framework for all participants.

17. The *Privacy Act 1988* (Cth) (Privacy Act) and the Australian Privacy Principles (APPs) apply to 'APP entities', primarily being Australian Government agencies and organisations with an annual turnover of more than $3 million. Consistency in regulation across jurisdictions reduces compliance burdens, reduces costs and provides clarity and simplicity for regulated entities and the community. National consistency, therefore, is a key goal of privacy and information sharing regulation.

18. However, a challenge associated with the system's legislative expansion is to ensure the application of privacy obligations to all participants, particularly given that some non-Commonwealth entity participants are not presently subject to the Privacy Act.

19. To address this issue, the Paper proposes that:

- the legislation will allow State and Territory entities with existing privacy regimes to participate in the system where their respective legislation confers privacy protection equivalent to the Commonwealth Privacy Act
- State and Territory entities operating without equivalent privacy legislation will be treated as organisations under s 6F of the Privacy Act to the extent required for activities related to

participation in the system.[2] This approach would result in the entities being bound by the APPs and other provisions of the Privacy Act where they are engaged in the system

- where private sector entities do not currently meet the revenue threshold under the Privacy Act, the legislation or Operating Rules will include requirements for them to be subject to 'equivalent protections in the Privacy Act'.[3] Under s 6EA of the Privacy Act, businesses can choose to be treated as an organisation for the purposes of the Privacy Act.

20. The OAIC supports the proposed expansion of the types of entities that would be subject to the Privacy Act. This addresses the privacy risks by regulating information handling practices that would otherwise be occurring outside the remit of the Privacy Act. It also presents an opportunity to establish measures that achieve equivalency and provides effective redress mechanisms for individuals where this might be might not otherwise available.

21. National consistency would also ensure that participants are required to abide by the Notifiable Data Breach (NDB) scheme. The key objective of the NDB scheme is to enable individuals whose personal information has been compromised in a data breach to take remedial steps to lessen the adverse impact that might arise from the breach. By arming individuals with the necessary information, they will have the opportunity to take appropriate action, such as monitoring their accounts and credit reports or taking preventative measures such as changing passwords and cancelling credit cards. The NDB scheme also serves the broader purpose of enhancing entities' accountability for privacy protection.

22. As an example of a similar legislative construct, the OAIC highlights its support for a regime of legislative equivalence proposed by the Data Availability and Transparency Bill 2020. This Bill is currently before Parliament and requires data scheme entities to be covered by the Privacy Act or a law of a State or Territory that provides for all of the following:

- protection of personal information comparable to that provided by the APPs
- monitoring of compliance with the law
- a means for an individual to seek recourse if the individual's personal information is mishandled.[4]

23. The Data Availability and Transparency Bill 2020 also provides that Australian Government agencies remain responsible for complying with the requirements of the NDB scheme in relation to any personal information that they have shared under the Data Availability and Transparency scheme. This is an important part of ensuring equivalency, given that no State or Territory privacy laws currently include a data breach reporting scheme.

24. In relation to small businesses operators and the proposed accreditation requirement that they seek to be treated as on organisation for the purposes of the Privacy Act, an alternative

[2] Section 6F allows for the making of regulations prescribing a State or Territory or instrumentality of a State or Territory (except certain instrumentalities) as an organisation for the purposes of the Privacy Act.

[3] Consultation Paper, s 6.3.3.

[4] Data Availability and Transparency Bill 2020, cl. 28, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6649

consideration is to amend s 6E of the Privacy Act to ensure acts and practices of small business operators engaging in the system are covered by the Privacy Act.

25. This would work in a manner similar to the way that the activities of a reporting entity or authorised agent under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* and its regulations and rules are bound by the Privacy Act. The OAIC considers this the preferable option, as it would mean that small businesses operators would not be required to opt-in under s 6EA but would be automatically subject to the Privacy Act by virtue of their activities.

Recommendation 3 - Small business operators are subject to the jurisdiction of the Privacy Act by an amendment to s 6E of the Privacy Act, rather than an obligation to elect to be treated as on organisation.

Defining Digital Identity information

26. The Paper seeks views on whether the proposed legislation should include a definition of Digital Identity information, or whether it is preferable to rely on the definitions of personal, sensitive, or protected information in other Commonwealth Acts.

27. The OAIC recommends reliance on the definitions of personal and sensitive information contained in s 6 of the Privacy Act. This approach builds upon an existing lexicon which will be familiar to many of the entities using the system, and is supported by well socialised interpretive guidance, therefore avoiding regulatory duplication and possible confusion.

Recommendation 4 –The existing definitions of personal and sensitive information, as set out in the Privacy Act, should be relied upon.

Age

28. The Paper seeks views on whether the proposed legislation should specify an age requirement to participate in the system. The OAIC recommends aligning the approach to that taken in the Privacy Act.

29. The Privacy Act protects an individual's personal information regardless of their age, and does not specify an age after which an individual can make their own privacy decision. For their consent to be valid, an individual must have capacity to consent.

30. An organisation or agency handling the personal information of an individual under the age of 18 must decide if the individual has the capacity to consent on a case-by-case basis. As a general rule, an individual under the age of 18 has the capacity to consent if they have the maturity to understand what is being proposed. If they lack maturity it may be appropriate for a parent or guardian to consent on their behalf.

31. OAIC guidance provides that if it is not practical for an organisation or agency to assess the capacity of individuals on a case-by-case basis, as a general rule, an organisation or agency may

assume an individual over the age of 15 has capacity, unless there is some uncertainty regarding the individual's capacity to understand.[5]

Recommendation 5 – An individual's capacity is assessed on a case-by case basis, but is it presumed that a person aged 15 years of over the has the capacity to consent, unless there is evidence to suggest otherwise.

Handling of biometric information

32. The OAIC recognises the benefits associated with expanding the system's use of biometric information. This includes enhancing convenience, efficiency and Digital Identity security. 'Biometric information' and 'biometric templates' are classified as 'sensitive information' under the Privacy Act,[6] and are afforded a higher level of privacy protection than other personal information. This reflects that inappropriate handling of sensitive information can have significant adverse consequences for an individual.

33. The Paper proposes that the safeguards around the use of biometric information include:

- an oversight regime for the use of biometric information
- limiting the use of biometric information to permitted purposes
- prohibiting the disclosure of biometric information to certain third parties, and for certain uses
- consent and deletion requirements for the use of biometric information.

34. The OAIC supports the DTA's proposal to complement protections set out in the Privacy Act by installing these additional safeguards.[7] As noted above the OAIC recommends that these safeguards remain in the primary legislation and suggests that the legislation exhaustively prescribe which types of biometrics are permissible for use in the system.

Privacy Impact Assessments

35. The TDIF accreditation process currently requires entities to conduct a privacy impact assessment (PIA) as part of the accreditation process. A PIA is a systematic written assessment of an activity or function that identifies the impact that the activity or function might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. Undertaking a PIA assists APP entities to build privacy considerations into the design of a project and achieve the project's goals while minimising the negative and enhancing the positive privacy impacts. A PIA can also help to build the community's trust that

[5] See sections are B.56-B.58 of the Australian Privacy Principles Guidelines – Chapter B: Key concepts': https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/

[6] Privacy Act, s 6.

[7] See, for example, APP 6.2(a)(i), which requires the reasonably expected secondary use of sensitive information to be directly related to the primary purpose. See also APP 11, which requires APP entities to take such steps that are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

privacy risks have been identified, and protections embedded, at the design stage of a new project involving personal information handling.

36. As noted earlier in the submission, the OAIC recommends that the requirement to conduct a PIA be included in primary legislation, as opposed to either remaining in the TDIF accreditation requirements or being included in the Operating Rules.

4. Independent Oversight Authority

37. The OAIC understands the legislation will install a permanent, independent Oversight Authority body or bodies to oversee the system's governance. The Paper proposes that the Oversight Authority could monitor participant compliance with fraud, cyber security and privacy requirements across the system. The OAIC supports the DTA's commitment to ensuring that system and its uses are subject to a robust and independent regulatory framework.

38. Transparency, accountability, choice and control are central themes in the Privacy Act and the APPs. These themes correspond with the objectives of APP 1 to ensure that regulated entities are open and transparent about their information handling practices. Businesses and federal government agencies are required under APP 1.2 to take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs. This supports entities taking a privacy-by-design approach, implementing robust privacy governance processes, and being accountable for their handling of personal information.

39. We support the regulator of digital identity being independent and having the regulatory and enforcement powers necessary to ensure the integrity of the system. The OAIC also supports the proposed accountability measures, such as the requirement for there to be periodic review of the legislation and of the Oversight Authority' performance and operation.

40. The OAIC recommends that it be empowered to oversee and enforce the privacy aspects of the system, as set out in the legislation, by being designated an Oversight Authority. This would be in addition to the OAIC exercising its regulatory oversight functions under the Privacy Act. The OAIC considers that this would avoid a fragmented approach to privacy oversight across the different sectors using the system and prevents duplication of regulatory oversight given the OAIC's existing privacy role in relation to many participants in the system. The increased functions resulting from designation as an Oversight Authority will also have resourcing implications for the OAIC which will need to be considered.

41. Additionally, the OAIC supports:

- proposed accountability measures, such as the requirement for periodic reviews of the legislation and of the Oversight Authority' performance and operation
- transparency mechanisms such as the publishing of an annual report detailing data breaches, PIAs and accuracy rates of biometric algorithms, among other things, to assure individuals that there is adequate oversight of how their personal information is being handled
- the establishment of a Privacy Advisory Committee.

Recommendation 6 – The OAIC is designated as the Oversight Authority for the privacy aspects of the system.

5. Trust marks

42. The OAIC supports the introduction of a legislated trust mark to signify TDIF accreditation to users. The OAIC considers that a certification scheme, such as a trust mark administered by an independent third party, could assist in ensuring that regulated entities are meeting their obligations under the system.

43. A trust mark offers benefits to consumers by providing them with evidence-based information which enables them to quickly assess the level of data protection offered by participants. It is also beneficial for participants insofar as it may garner User's trust, thereby granting a competitive advantage over non-certified entities.

44. Several jurisdictions around the world, including Japan,[8] New Zealand,[9] and Singapore[10] have implemented privacy certification schemes. The OAIC suggest that the DTA consider these schemes to model a trust mark certification scheme suitable for the Australian operational environment.

[8] More information about Japan's PrivacyMark System can be found at https://privacymark.org/

[9] More information about New Zealand's Privacy Trust Mark can be found at https://www.privacy.org.nz/resources-2/applying-for-a-privacy-trust-mark/

[10] More information about Singapore's Data Protection Trustmark can be found at https://www.imda.gov.sg/programme-listing/data-protection-trustmark-certification