Australian Government
Office of the Australian Information Commissioner

Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023: Submission to Senate Economics Legislation Committee

Submission by the Office of the Australian Information Commissioner

Angelene Falk
Australian Information Commissioner and Privacy Commissioner
19 January 2024

OAIC

Australian Government
Office of the Australian Information Commissioner

Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023: Submission to Senate Economics Legislation Committee

Submission by the Office of the Australian Information Commissioner

Angelene Falk
Australian Information Commissioner and Privacy Commissioner
19 January 2024

OAIC

January 2024

Contents

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the Committee's inquiry into the *Digital ID Bill 2023* (Digital ID Bill) and *Digital ID (Transitional and Consequential Provisions) Bill 2023* (Transitional and Consequential Provisions Bill).

2. The OAIC has engaged extensively with the Department of Finance (the Department), Attorney-General's Department and Digital Transformation Agency (DTA) throughout the development of the Trusted Digital Identity Framework[1] and the draft Digital Identity legislation. We have made submissions to four previous consultations, including the Department's recent consultation on exposure drafts of the Digital ID Bill and Digital ID Rules.[2]

3. The OAIC is supportive of the Digital ID Bill and the Transitional and Consequential Provisions Bill and welcomes our proposed role as the independent privacy regulator for the scheme. When accompanied by strong statutory safeguards and robust regulatory oversight, digital identity systems have the potential to improve privacy protections by minimising the collection and use of personal information by businesses and government agencies, and giving individuals greater security and control over their identification documents and credentials.

4. In establishing a legislative framework for Digital ID in Australia, the Digital ID Bill contains strong privacy protections, which include privacy safeguards that will operate alongside existing protections under the *Privacy Act 1988* (Cth) (Privacy Act). These protections are critical to improving user safeguards, addressing areas of potential privacy risk, and building community trust and confidence in the Australian Government Digital ID System (AGDIS) to encourage the uptake of Digital ID.

5. This submission provides a brief overview of the privacy protections in the Digital ID Bill, the proposed role of the OAIC in the Digital ID framework, the OAIC's engagement with the Bills to date and recommends areas for further consideration and amendment.

Privacy protections

6. The Privacy Act and Chapter 3 of the Digital ID Bill provide a legislative framework for the protection of personal information within the Digital ID system. The Bill requires all entities accredited under the Digital ID system to either:

    - be subject to the Privacy Act
    - be subject to a State or Territory privacy law that provides for all of the following:
        - protection of personal information comparable to that provided by the Australian Privacy Principles (APPs);

[1] Australian Government, 'Trusted Digital Identity Framework (TDIF)', accessed 3 January 2024.

[2] OAIC, *Digital Identity Legislation Consultation Paper*, Submission to the Digital Transformation Agency (DTA), 18 December 2020; OAIC, *Digital Identity Legislation Position Paper*, Submission to the DTA, 15 July 2021; OAIC, *Trusted Digital Identity Bill legislative package: exposure draft consultation*, Submission to the DTA, 27 October 2021; OAIC, *2023 Digital ID Bill and Digital ID Rules*, Submission to the Department of Finance, 17 October 2023.

- monitoring of compliance with the law; and
- a means for an individual to seek recourse if their personal information is dealt with in a way contrary to the law; or

- have entered into an 'APP-equivalent agreement' with the Commonwealth that requires compliance with the Australian Privacy Principles (APPs).[3]

7. Accredited entities will be required to comply with the additional privacy safeguards in Chapter 3, Part 2, Division 2. Any contravention of these safeguards will constitute an interference with the privacy of an individual for the purposes of the Privacy Act. All accredited entities will also have to comply with the Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act, unless they are covered by a comparable State or Territory scheme.[4]

8. The OAIC supports the proposed privacy framework for the Digital ID system. In applying to all accredited entities, the additional privacy safeguards and notifiable data breach requirements promote a consistent level of privacy protection.

OAIC role in the Digital ID framework

9. Under the Digital ID Bill, the Information Commissioner will have regulatory oversight and functions in relation to:

- the additional privacy safeguards set out in Chapter 3, Part 2, Division 2 – a contravention of these safeguards by an accredited entity will constitute an interference with the privacy of an individual for the purposes of the Privacy Act[5]
- the privacy-related terms of an APP-equivalent agreement[6]
- the Notifiable Data Breaches (NDB) scheme under Part IIIC of the Privacy Act, in relation to accredited entities that would not otherwise be covered by the Privacy Act or a comparable State or Territory scheme[7]
- providing advice, on request by the Digital ID Regulator, on matters relating to the operation of the Digital ID Act[8] and
- undertaking assessments of whether personal information is being maintained and handled in accordance with the additional privacy safeguards and the privacy requirements in APP-equivalent agreements.[9]

---

[3] Digital ID Bill, subclause 36(2).

[4] Digital ID Bill, clause 40.

[5] Digital ID Bill, clause 38.

[6] Digital ID Bill, clause 37.

[7] Digital ID Bill, clause 40.

[8] Digital ID Bill, clause 42.

[9] Transitional and Consequential Provisions Bill, Schedule 2, clause 6.

10. The OAIC welcomes the proposed regulatory role of the Information Commissioner under the Digital ID Bill. Strong and consistent privacy regulation is critical to safeguarding the privacy foundations of the Digital ID system and securing consumer trust and confidence.

Previous OAIC submissions – Digital ID Bill

11. In our submission to the exposure draft public consultation, the OAIC made a number of general recommendations to enhance the Digital ID Bill by clarifying the scope of the Information Commissioner's role and strengthening our ability to effectively enforce privacy breaches in the Digital ID system.[10]

12. While the latest iteration of the Digital ID Bill has been enhanced and contains strong privacy protections, we recommend the Committee consider the following points based on our previous submission in its review of the Bill which would further improve the system's privacy regime that:

    a. the Bill outline a clear process for determining whether a State or Territory privacy law or data breach notification scheme is comparable to the federal Privacy Act[11]

    b. the Bill make the destruction and de-identification requirement in clause 136 an additional privacy safeguard in Chapter 3, Part 2, Division 2, regulated by the Information Commissioner[12]

    c. clause 136 provide greater specificity regarding retention of personal information[13] and

    d. greater consistency in privacy regulation could be achieved if accredited State and Territory entities were prescribed under section 6F of the Privacy Act.[14]

Additional points for consideration and amendment

13. The OAIC notes that clause 54 has been amended following the public consultation to narrow the circumstances in which certain personal information may be disclosed to an enforcement body. The OAIC is supportive of the narrowing of this provision, but notes that there may be an inconsistency between clause 54 and paragraph 47(4)(e), which permits the disclosure of unique

---

[10] OAIC, *Digital Identity Legislation Consultation Paper*, Submission to the Digital Transformation Agency (DTA), 18 December 2020; OAIC, *Digital Identity Legislation Position Paper*, Submission to the DTA, 15 July 2021; OAIC, *Trusted Digital Identity Bill legislative package: exposure draft consultation*, Submission to the DTA, 27 October 2021; OAIC, *2023 Digital ID Bill and Digital ID Rules*, Submission to the Department of Finance, 17 October 2023.

[11] As required by paragraphs 36(2)(b) and 40(2)(b). An express mechanism for determining equivalency may provide greater clarity for accredited entities and regulators as to the regulatory scheme applicable to a particular accredited entity.

[12] Given the potential regulatory overlap between clause 136 and APP 11.2, the OAIC considers that including this as an additional privacy safeguard, regulated by the Information Commissioner, would remove the risk of inconsistent interpretations of an entity's destruction or de-identification obligations by the Digital ID Regulator and the Information Commissioner, and provide greater clarity for accredited entities.

[13] The current drafting of clause 130 may lack the necessary degree of certainty to ensure data security risks are effectively mitigated, particularly because the clause defers to other laws and court/tribunal orders for retention requirements.

[14] Section 6F is a mechanism which allows the Governor-General to make regulations prescribing a State or Territory entity, so that the Privacy Act applies as if the entity were an organisation.

identifiers for the purpose of detecting, reporting, investigating or prosecuting an offence against a law of the Commonwealth, a State or Territory. We recommend the Committee consider removing paragraph 47(4)(e) from the Bill or alternatively, revising paragraph 47(4)(e) to align it with the relevant law enforcement exceptions under paragraph 54(1)(b).

14. Clause 84 of the Digital ID Bill provides for the protection of accredited entities from civil or criminal liability in certain circumstances, including where they have provided (or not provided) an accredited service in good faith and in compliance with the Digital ID Act.[15] It is not clear how this provision, as currently drafted, will interact with an accredited entity's obligations under other laws, including the Privacy Act and APPs. We suggest the provision is clarified to avoid any unintended exclusion of Privacy Act requirements for accredited entities.

15. We also note that under the Digital ID Bill, small businesses seeking accreditation will be required to opt in to Privacy Act coverage under section 6EA of that Act. We consider that an alternative mechanism for bringing accredited non-APP entities within the scope of the Privacy Act would be more administratively efficient, both for the OAIC and the relevant entity. For example, subsection 6E(1D) of the Privacy Act provides for automatic coverage of small business operators accredited under the Consumer Data Right.[16]

Transitional and Consequential Provisions Bill

16. The Transitional and Consequential Provisions Bill suspends the requirement for the Minister to consult on the making or amending of rules for the first 6 months after the Bill's commencement.[17] While we note that exposure drafts of the Digital ID Rules and Digital ID Accreditation Rules were already released for public consultation (giving the OAIC the opportunity to be consulted) in September 2023, the OAIC recommends that we should be consulted before the making or amending of any rules that relate to privacy, including in the first 6 months after commencement.

[15] Digital ID Bill, paragraph 84(1)(a).

[16] The OAIC has previously suggested that an amendment to section 6E would be preferable to requiring small businesses to opt in to Privacy Act coverage, as it would ensure such entities were automatically subject to the Privacy Act by virtue of their activities reducing administrative burden on small businesses and the OAIC: OAIC, *Digital Identity Legislation Consultation Paper*, Submission to the DTA, 18 December 2020.

[17] Transitional and Consequential Provisions Bill, Schedule 1, clause 9. This temporarily suspends the Minister's consultation obligation under clause 169 of the Digital ID Bill, which applies to the making or amending of rules under clause 168.