Australian Government
Office of the Australian Information Commissioner

Senate Legal and Constitutional Affairs Legislation Committee inquiry into the Identity Verification Services Bill 2023 and Identity Verification Services (Consequential Amendments) Bill 2023

Submission by the Office of the Australian Information Commissioner

Angelene Falk
Australian Information Commissioner and Privacy Commissioner
4 October 2023

OAIC

Summary of recommendations

The Office of the Australian Information Commissioner (OAIC) provides the following recommendations to build upon and enhance the privacy protections contained in the *Identity Verification Services Bill 2023* (IVS Bill)*:*

Recommendation 1: Amend the IVS Bill to include a provision that will make a breach of a participation agreement an interference with privacy under the *Privacy Act 1988* (Privacy Act), enabling enforcement by the OAIC under the Privacy Act for Australian Privacy Principle (APP) entities.

Recommendation 2: Amend the IVS Bill to provide that 'identification information' as defined in clause 6 of the bill is personal information for the purposes of the Privacy Act.

Recommendation 3: The IVS Bill should provide that participation agreements must be privacy-enhancing and consistent with the APPs.

Recommendation 4: That the IVS Bill clarifies that the compliance obligations under it do not alter a participating entity's obligations under the Privacy Act.

Recommendation 5: Amend clause 40 of the IVS Bill to enliven the OAIC's existing assessment powers in s 33C(1) of the Privacy Act in relation to the annual assessment requirement, or alternatively, reframe the assessment as an advice and annual reporting requirement.

Recommendation 6: Amend the IVS Bill to include a disclosure of protected information provision to the Information Commissioner for the purposes of exercising a relevant function or power, similar to that provided in the bill for the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman.

Recommendation 7: (a) For State and Territory participants, consideration should be given to the adequacy of State and Territory privacy legislation and whether any specific additional protections are needed for these participants (for example, requiring them to opt-in to coverage of the Privacy Act).

(b) Alternatively, the IVS Bill should be amended to require participation agreements to contain NDB-like obligations to notify the Commissioner and individuals where the entity is not covered by the NDB scheme or a State/Territory equivalent.

Recommendation 8: The rule making provisions at clause 44 of the IVS Bill should include a mandatory requirement to consult with the Commissioner in the development of any rules made under the bill.

Introduction

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the Committee's inquiry into the *Identity Verification Services Bill 2023* (IVS Bill) and *Identity Verification Services (Consequential Amendments) Bill 2023*.

2. The IVS Bill will establish a legislative framework for the operation of existing identity verification services, the Document Verification Service (DVS), Face Verification Service (FVS) and National Driver License Facial Recognition Solutions (NDLFRS). The OAIC broadly supports the bill which will provide important privacy and security protections for individuals while ensuring governments and industry can continue to use these vital identity verification services. The OAIC further supports the restrictions placed on 1:many matching, given the significant privacy impacts of this type of matching.

3. As set out in the draft explanatory memorandum, the IVS Bill provides a multi-faceted approach to the protection of privacy. This approach includes requirements that entities using the services must be subject to a relevant privacy law (either the *Privacy Act 1988* (Privacy Act), or State and Territory legislation), and comply with a range of additional privacy and security-related requirements under the relevant participation agreements.

4. The bill also contains a number of transparency and oversight measures including requirements to publish participation agreements and other relevant policies, annual reporting requirements to parliament, provisions to support oversight by the Inspector-General of Intelligence and Security (IGIS) and the Commonwealth Ombudsman, and an annual assessment by the Australian Information Commissioner (Information Commissioner).

5. Within this context, this submission makes a number of observations and recommendations to clarify the OAIC's position as the independent national privacy regulator and enhance the privacy protection mechanisms in the IVS Bill.

Privacy safeguards and oversight

6. By way of overall comment, we consider that the IVS Bill should clearly set out the OAIC's regulatory role, including clear enforcement mechanisms, to ensure that the Information Commissioner can efficiently and effectively carry out their oversight functions.

7. This is particularly relevant in relation to the enforcement of the participation agreements, which are one of the key additional privacy protection mechanisms in the IVS framework. We understand that all entities using the services will be required to be a party to a participation agreement,[1] and a precondition for entering such an agreement will be being subject to either

[1] Participation agreements will set out a range of privacy safeguards including procedures relating to the obtaining of consent for the collection, use and disclosure of personal information under the services, and placing limitations on further on-disclosure of personal information by the collecting entity.

the Privacy Act or a State/Territory privacy law, or otherwise having agreed to comply with the Australian Privacy Principles (APPs).[2]

8. While we support these additional protections, the bill does not provide a clear framework for the OAIC to enforce these agreements. Where participating entities may be subject to the Privacy Act, any enforcement activity by the OAIC in relation to a breach of a participation agreement (including any ability to investigate individual complaints) would need to be through the ordinary mechanisms of the APPs/Privacy Act. However, a breach of a participation agreement may not necessarily be a breach of the Privacy Act, even where the agreement clearly sets out privacy-related safeguards. We also note the OAIC would have no ability to enforce breaches of participation agreements in relation to State and Territory entities.

9. We understand the consequence for breaching a participation agreement[3] is the possible termination or suspension of access to the matching facilities. The OAIC notes that in practice it may be difficult to use this enforcement measure, especially in relation to participants who provide essential services to the community.

10. We consider it would be more appropriate to include a provision in the IVS Bill that will make certain (privacy-related) breaches of a participation agreement (for example, breaches of provisions required by clauses 9(2), 10 or 11 of the bill) an interference with privacy under the Privacy Act. This could be done, for example, by making such a breach an interference with the privacy of an individual (see s 13 of the Privacy Act). This will clearly enable enforcement (including the ability to deal with complaints) by the OAIC under the Privacy Act in relation to entities with a participation agreement.

11. Finally, for clarity and to support the operation of clear enforcement and oversight mechanisms, we consider that the IVS Bill should be amended to provide that 'identification information' as defined in clause 6 of the bill is personal information for the purposes of the Privacy Act.

Recommendation 1: Amend the IVS Bill to include a provision that will make a breach of a participation agreement an interference with privacy under the Privacy Act, enabling enforcement by the OAIC under the Privacy Act for APP entities.

Recommendation 2: Amend the IVS Bill to provide that 'identification information' as defined in clause 6 of the bill is personal information for the purposes of the Privacy Act.

[2] See subclause 9(1) of the IVS Bill

[3] or a National Drivers Licence Facial Recognition Solution (NDLFRS) agreement

Participation agreements and interactions with the APPs

12. The IVS Bill provides an explicit basis for the collection, use and disclosure of information for the purposes of the three approved matching activities. However, it also provides that the participation agreements must impose specified additional requirements in relation to a participant's handling of personal information, including in relation to obtaining consent (for example, see clauses 9(2)(c) and 9(3) of the IVS Bill).

13. The OAIC therefore recommends that the IVS Bill clarifies how any privacy-related requirements contained in the participation agreements are intended to interact with the APPs. For example, the IVS Bill could state that participation agreements are intended to be privacy-enhancing and may therefore impose additional requirements to the APPs, but any such requirements must not be contrary to, or inconsistent with, the APPs.

14. The IVS Bill should also generally clarify that the compliance obligations under it do not alter entities' obligations under the Privacy Act, and in particular the general obligation to notify the OAIC of eligible data breaches.

Recommendation 3: The IVS Bill should provide that participation agreements must be privacy-enhancing and consistent with the APPs.

Recommendation 4: That the IVS Bill clarifies that the compliance obligations under it do not alter a participating entity's obligations under the Privacy Act.

Annual assessments by the OAIC

15. The OAIC notes that the assessment provisions at clause 40 are unusual in that they do not activate the OAIC's usual assessment regulatory powers.[4] The OAIC would therefore be reliant on information agreed to be provided by the department when carrying out this specific annual function.

16. Noting the assessment is one of the key privacy assurance mechanisms in the framework, and given our role as the independent national privacy regulator, the OAIC considers that clause 40 needs to provide the Information Commissioner with the ability to discharge the assessment function in a manner that is appropriately independent. The model as drafted would also likely be inconsistent with public expectations in relation to the oversight, transparency and accountability for the IVS system, given the significant privacy impacts for individuals.

17. The OAIC therefore considers that a more appropriate approach to ensuring transparency and accountability in the IVS system would be to align the assessment requirements in the IVS Bill

[4] Such as the power to compel information from the department, or to enter premises to inspect systems.

with the OAIC's usual assessment powers as set out in s 33C of the Privacy Act.[5] Amongst other things, s 33C of the Privacy Act provides a power to require an entity to give information or produce documents relevant to the assessment, without reliance on the agreement of the entity.

18. Providing the OAIC with discretion as to the scope, timing and focus of an assessment allows the OAIC to undertake the function in relation to areas of most significant privacy risk. As set out in the OAIC's Guide to Privacy Regulatory Action, an assessment can be either risk-based (that is, forward looking, and focussed on identifying risks and making best-practice recommendations) or compliance based and the OAIC has significant flexibility and experience in how it carries out this established function.

19. Alternatively, the provision could be reframed as an advice and annual reporting requirement. Under such a clause the Information Commissioner could provide regulatory advice on request to the Secretary of the Attorney-General's Department about privacy matters related to the operation and management of the approved identity verification facilities. Similar to clause 41, the Commissioner could then be required to provide a written report to the Secretary at the end of the financial year that includes information about the advice provided, complaints received and resolved, investigations commenced and completed as well as information about any data breaches notified. The OAIC would still be able to use its usual assessment and other regulatory powers under the Privacy Act, in relation to the use of the relevant services.[6]

Recommendation 5: Amend clause 40 of the IVS Bill to enliven the OAIC's existing assessment powers in s 33C(1) of the Privacy Act in relation to the annual assessment requirement, or alternatively, reframe the assessment as an advice and annual reporting requirement.

Protected information framework

20. To ensure the efficient operation of the Information Commissioner's oversight role and enforcement powers, we recommend that the IVS Bill be amended to include a disclosure of protected information provision to the Information Commissioner, similar to that provided for the IGIS and Commonwealth Ombudsman at clauses 33 and 34 of the IVS Bill.

Recommendation 6: Amend the IVS Bill to include a disclosure of protected information provision to the Information Commissioner for the purposes of exercising a relevant function or

[5] This could be done by amending clause 40 of the bill to align the annual OAIC assessment with the approach taken in s 33C(1) of the Privacy Act, or by amending the Privacy Act to include a general power for the Information Commissioner to assess the approved identity verification facilities.

[6] For example, the OAIC would be able to conduct an assessment under s 33C of the Privacy Act. However, these powers would apply only in relation to potential breaches of the APPs by entities regulated by the Privacy Act, and would not need to be conducted annually (rather, the OAIC would consider whether any specific regulatory action was required, in accordance with the OAIC's usual approach as outlined in the *Privacy regulatory action policy*).

power, similar to that provided in the bill for the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman.

State and Territory participants

21. As State and Territory government participants are not subject to the Privacy Act, further consideration may need to be given to the comparability of State and Territory privacy legislation where this is a requirement for participation in the use of a matching service, with a view to considering whether any specific additional protections are needed for those participants.

22. In particular, where there is no relevant NDB legislation in a jurisdiction, we recommend relevant entities be required to comply with additional requirements including notifying the Information Commissioner and individuals in the event of an eligible data breach, in addition to the requirements in the bill to notify the Department. This would not be enforceable by the OAIC, but would provide additional transparency for individuals in the event of data breach.

Recommendation 7: (a) For State and Territory participants, consideration should be given to the adequacy of State and Territory privacy legislation and whether any specific additional protections are needed for these participants (for example, requiring them to opt-in to coverage of the Privacy Act).

(b) Alternatively, the IVS Bill should be amended to require participation agreements to contain NDB-like obligations to notify the Commissioner and individuals where the entity is not covered by the NDB scheme or a State/Territory equivalent.

Rule-making powers

23. Clause 44 of the IVS Bill contains a rule making power for the Minister to, by legislative instrument, make rules prescribing matters required or permitted by the bill, or necessary or convenient for carrying out or giving effect to the bill. As part of this, the Minister may make rules to prescribe equivalent privacy laws (for the purposes of enabling an entity to meet its general obligations under a participation agreement), or to prescribe a particular government entity as one which is eligible to enter into a participation agreement.[7]

24. As previously recommended in the OAIC's submission to the PJCIS inquiry into the Identity-matching Services Bill 2018 (IMS Bill), we consider there should be a mandatory requirement to consult with the Information Commissioner in the development of any rules made under the IVS Bill, given the potential privacy impacts.

[7] See subclause 9(1) of the IVS Bill

Recommendation 8: The rule making provisions at clause 44 of the IVS Bill should include a mandatory requirement to consult with the Commissioner in the development of any rules made under the bill.