Electronic Identity Verification Bill

Submission by the Privacy Commissioner

to the Government Administration Committee

---

30 March 2012

Privacy Commissioner
Te Mana Matapono Matatapu

P/0114 /A278185

1. Introduction

1.1. I support passage of the Electronic Identity Verification Bill because it puts in place a robust legal framework for the operation of the Identity Verification System (IVS), and places control over information firmly in the hands of users.

1.2. Maintaining users' control over their personal information is critical to the success of the IVS. If the IVS is to be widely adopted, and therefore to provide value to participating agencies, users must have trust that their information will be protected, and that they have control over when it is used to establish their identity.

1.3. The service is intended to make accessing government services easier by making it simpler for individuals to assert their identity. It should also reduce the potential for others to fraudulently use another individual's identity.

1.4. Key privacy provisions are found throughout the Bill. The most critical in my view are that:

- the operation of the system is based on consent at every key point
- agencies cannot make use of the IVS the only means for establishing identity
- the Bill overrides the Privacy Act only where it is necessary to do so, and puts in place a robust alternative regime where it does; and
- I am able to request regular reporting from DIA on the operation of the system.

It is essential that those privacy protections are maintained.

1.5. There are two minor improvements that could be made to the Bill to further clarify its relationship to the Privacy Act. The first of these relates to the Chief Executive's responsibilities under the Privacy Act, when a correction is requested to information, while the second ensures that the Bill is crystal clear about an individual's ability to lodge a complaint with my Office.

1.6. My positive attitude to the Bill is reinforced by the efforts that have been made to identify and address privacy risks in the design of the IVS system itself. Throughout the development process, a number of privacy impact assessments have been carried out by independent parties. In addition, DIA has involved my office throughout the development of the proposed system.

2. List of Recommendations

Recommendation A
I recommend that clause 26(5), relating to an application to amend an electronic identity credential, be amended to read:

(5) If the chief executive refuses the application, he or she must –
(a) as soon as practicable, give the applicant written or electronic notice of the decision and the reason for it; and

(b) if so requested by the applicant, take such steps (if any) as are reasonable to attach to the credential a statement of the correction sought or otherwise indicate that the information is contested.

Recommendation B
I recommend that clause 61, relating to protection from liability, be amended to read

(5) To avoid doubt, subsection (1) does not limit an individual's ability to make a complaint to the Privacy Commissioner alleging that any action is or appears to be an interference with the privacy of an individual.

3. Trust and consent are central to the IVS's success

3.1. The success of the IVS depends on a large number of New Zealanders making use of it on a regular basis. People will only use the IVS if they are confident that their information will be protected, and they have control over how it is used.

3.2. The Bill's use of consent as the basis for the IVS is therefore central to the wide adoption of the system. Clause 4(1)(d) permits the IVS to supply information to an agency only with the individual's consent. This is the only basis on which the IVS could be successful in its aims.

3.3. Clause 4(1)(b), which prevents agencies from making the IVS the only means by which individuals can verify their identity, is also important. Any sense that an agency was attempting to coerce users into using the IVS would most likely discredit the system as a whole, and hinder uptake. Not all users will be able to make use of an online system. In some circumstances users may prefer not to use an online channel for providing identity information (for instance because they need to explain the information face to face).

4. Application of the Privacy Act 1993

4.1. The Bill overrides the Privacy Act only where it is necessary to do so and emphasises the continuing application of the Privacy Act in the operation of the IVS. This is important for establishing individuals' trust that their personal information will be protected.

4.2. Clause 55 sets out the Bill's relationship to the Privacy Act, and lists two key exceptions:

- It overrides principle 11 (which prohibits disclosure of information other than for the purpose for which it was collected) in favour of the Bill's own tighter rules about disclosure of personal information
- It allows for retention of information from information matches in clause 36(2), contrary to the Privacy Act's information matching rules

4.3. The override of principle 11 of the Privacy Act does two things. First, it reinforces that the disclosures of identity information necessary for the IVS to function must occur only with the consent of the individual. Second, it overrules the Privacy Act's exceptions to principle 11 in favour of a regime that is more appropriate to the IVS itself.

4.4. The situations in which disclosure of information in the IVS is allowed, such as for law enforcement or court proceedings, are set out in clause 21. These rules are more restrictive than those found in the Privacy Act and apply only to access to an individual's usage history, and not the nature of their transactions. This is entirely appropriate for a system that can be seen as holding a potentially comprehensive record of when an individual has interacted with government agencies.

4.5. The information retention provisions outlined for information matching in clause 36(2) enable the IVS to comply with auditing requirements. I believe that this justification for keeping and maintaining information is acceptable, particularly given that these audit requirements will help prevent identity theft, and will therefore directly benefit users. Rule 6 of the information matching provisions would be unnecessarily restrictive in this context.

4.6. In all other respects, the Privacy Act continues to govern the use of personal information by the IVS. In particular, subclause 55(3) ensures that any improper disclosure of information will still be considered a breach of an information privacy principle.

5. Application for amendment – Statement of correction

Recommendation A
I recommend that clause 26(5), relating to an application to amend an electronic identity credential, be amended to read:

(5) If the chief executive refuses the application, he or she must –
(a) as soon as practicable, give the applicant written or electronic notice of the decision and the reason for it; and
(b) if so requested by the applicant, take such steps (if any) as are reasonable to attach to the credential a statement of the correction sought or otherwise indicate that the information is contested.

5.1. One potential inconsistency between the Privacy Act and the Bill is that the Bill's proposed procedure for amending an electronic identity credential in clause 26 does not include an obligation to attach a statement of correction to personal information where an individual claims the information is incorrect, but the agency does not agree.

5.2. Clause 26 sets out the application process and the chief executive's decision-making obligations and powers. Under the Privacy Act the chief executive also has an obligation to attach a statement of correction to the information if an application for amendment is refused, and the applicant requests it. For the sake of clarity, I propose that this obligation be made explicit in the amendment procedure.

6. Protection from liability – Relationship with the Privacy Act

Recommendation B
I recommend that clause 61, relating to protection from liability, be amended to read

(5) To avoid doubt, subsection (1) does not limit an individual's ability to make a complaint to the Privacy Commissioner alleging that any action is or appears to be an interference with the privacy of an individual.

6.1. I am concerned that clause 61 of the Bill may make an individual's ability to lodge a privacy complaint with my office about use of the IVS unclear. Clause 61 protects DIA from liability in the course of operating the IVS.

6.2. The public's ability to lodge complaints with my office is vital to keeping agencies accountable for good privacy practice. If this ability is in doubt, it can impact on the agency's trustworthiness in the public eye. The Bill specifically recognises this in clause 55, by making inappropriate disclosure of information subject to the Privacy Act, even though the Bill overrides principle 11.

6.3. I am mindful of the need to protect against fraudulent allegations, as well as the strength of the preceding offence clauses. I understand, however, that it is not the intent of clause 61 to prevent complaints being made to my office even though it may affect their subsequent consideration and whether damages are payable for any harm caused. I therefore recommend that the further subsection be added outlining that this clause does not affect the ability to lodge a complaint with my office.

7. Reporting and review powers

7.1. In recognition of the role of privacy and trust in the success of the IVS, the Bill provides me with two specific statutory powers:

- Under clause 52 of the Bill I may request regular reports from DIA on the operation of the IVS
- Under Schedule 1 of the Act I may request DIA to undertake a review of confirmation agreements.

7.2. My ability to request regular reports on the operation of the IVS will support the transparency and trustworthiness of the IVS by subjecting it to independent oversight. The breadth in scope of the reporting power is necessary to ensure that effective oversight of privacy considerations can be maintained.

7.3. Much of the privacy risk in the IVS occurs not at the legislative level, but at the level of operational and system design. Reporting powers will enable me to ensure that privacy remains a key consideration in the IVS's operation over the longer term.

7.4. It is also appropriate that we have oversight of confirmation agreements. Confirmation agreements govern the means by which individuals' identities are confirmed with other agencies. They have some similarities with the information matching provisions set out in clauses 33-36, which are subject to my oversight through the Privacy Act's information matching rules. The identity confirmation process represents a key part of the authentication chain.

8. Privacy by design

8.1. While I support this Bill, I am also reasonably confident that the design of the IVS itself limits and mitigates many of the potential privacy risks. The core of the IVS is the assertion of user identity. The use of personal information is key to making it work, and therefore privacy has been an integral part of the IVS from the start.

8.2. DIA has commissioned several privacy impact assessments (PIAs) from an expert external agency on the implementation of the IVS. The risks identified in the PIAs have formed part of a systematic process for addressing privacy risks, including regular meetings between my Office and DIA. Because of this attention to privacy, the IVS has been designed with responsible information collection and handling in mind.