

Privacy Commissioner's Submission to the Law and Order Committee on the Enhancing Identity Verification and Border Processes Legislation Bill 147-1

Executive summary

1. The Enhancing Identity Verification and Border Processes Legislation Bill ("the Bill") is an omnibus bill that amends the Privacy Act, Births, Deaths, Marriages and Relationships Registration Act, Immigration Act, Customs and Excise Act, Intellectual Disability (Compulsory Care and Rehabilitation) Act, Land Transport Act, Mental Health (Compulsory Assessment and Treatment) Act, Parole Act and the Sentencing Act. The Bill provides for increased information sharing, reflecting recommendations of the Government Inquiry into Matters Concerning the Escape of Phillip John Smith/Traynor ("the Inquiry").
2. I support the Inquiry's recommendations to improve identity management in the justice sector. The Bill gives effect to the Inquiry's recommendations through primary legislation and a schedule (Schedule 1) that may be amended by Order in Council. Schedule 1 states which agencies may share information for the purpose of identity verification and the agencies they may share it with.
3. The Bill does not reflect the suggestions I made to officials for improving transparency and oversight of the proposed regime. There are a number of areas where I consider additional safeguards should be included to ensure the legislation meets legitimate law enforcement needs while also providing the appropriate privacy safeguards and transparency mechanisms.
4. My recommendations, a summary of which is attached as an appendix, aim to help ensure the resulting legislation appropriately addresses the principles of oversight and transparency that are fundamental to the objectives of this Bill. My comments below are provided in the same order as the Bill.

Definition of biometric information

5. The definition of 'biometric information' contained in clause 24 (Immigration Act) is different to the definition contained in clauses 6 (Privacy Act) and 14 (Customs and Excise Act). I suggest the Committee consider aligning the definitions. Inconsistencies between statutes could lead to confusion as to what can and cannot be shared under the proposed regime.

Amendments to Privacy Act (clauses 3-8)

6. I was not consulted on the major policy proposals submitted to Cabinet that formed the basis for this Bill. This meant I was unable to provide comment on or seek clarification of the policy intent of the amendments to the Privacy Act 1993, in particular the addition of the new schedule, at the Cabinet stage.
7. The proposed Schedule 4A and Part 10A of the Privacy Act are potentially unnecessary and confusing, as these amendments would add to the information sharing legislative mechanisms already available to agencies. For example, the information sharing that the Schedule seeks to enable could be achieved through existing legislative means such as Approved Information Sharing Agreements (AISAs).
8. I therefore **recommend** the committee consider whether the Bill should proceed with Part 10A and the associated Schedule.
9. If the amendments to the Privacy Act are to proceed, I would make the following comments to improve these provisions.

Definition of identity information

10. Clause 6 of the Bill (new section 109C inserted) defines identity information as:

“in relation to an individual, means any information that identifies, or relates to the identity of, the individual, and includes (without limitation) the following information:

- (a) The individual’s biographical details (for example, the individual’s name, address, date of birth, place of birth, and gender):
- (b) The individual’s biometric information:
- (c) A photograph or visual image of the individual:
- (d) Details of the individual’s –
 - i. New Zealand travel document; or
 - ii. Certificate of identity:
- (e) Details of any distinguishing features (including tattoos and birthmarks)”

11. I **recommend** that the definition of ‘identity information’ be limited to the types of information contained in (a) – (e). The current definition is overly broad and creates the risk of information being shared that is of a type beyond what is intended by this Bill.

12. The Bill could be left open to interpretation that information such as DNA, health information, the name of a person's spouse or associates, work history or travel history are 'identity information', as this information 'relates to the identity' of a person. These types of information are outside the scope of what should be considered *identity information* and fit into a broader category of what might be considered *identifying information*. Further, the potential for DNA information to be shared as 'identity information' undermines the currently constrained definition of biometric information contained in the Bill.

Requirement to consult with the Office of the Privacy Commissioner

13. Clause 6 specifies the manner and form of access the Schedule 1 agencies may have to identity information. It states that agencies may have access "by direct access to information stored in a holder agency's database or by exchange of information between the agencies". However, the Bill does not specify what terms govern these arrangements.

14. I therefore **recommend** new section 109E (Manner and form of access) be amended to specifically include a requirement to consult the Privacy Commissioner on access arrangements. The amendment should insert "after consultation with the Privacy Commissioner", after the words "in a manner agreed by the agencies". I also **recommend** new section 109E be amended by inserting sub clause (3), which should state, "The Privacy Commissioner must also be consulted whenever an agreement is substantively amended".

15. Direct access to databases creates higher privacy risks than more controlled methods of exchanging information, and consultation with the Privacy Commissioner would help ensure that agencies have appropriate protections in place. Furthermore, due to the highly personal nature of biometric information it is essential that a privacy by design approach is taken by each agency collecting, holding and accessing such information. That is, an approach that deliberately incorporates privacy protections (for example, encryption, information handling processes, etc.) from the outset.

16. Consistent with Principle 3 of the Privacy Act and to promote transparency, I **recommend** that new section 109E mirror the requirements contained in section 95E of the Policing Act 2008. This would require agencies to make any access agreements publically available.

Amendments to Births Deaths, Marriages, and Relationships Registration Act

17. Clause 12 (new section 78AB inserted) allows for the sharing of birth, death, marriage and civil union information with certain agencies under specified circumstances which include if a person is detained or arrested. The clause does not specify the purpose for which this information may be sought.

18. The general intent of this Bill is to assist identity verification. I therefore **recommend** that the Bill state that the Registrar-General may share specified personal information with an agency for the purpose of verifying a person's identity in the case of (a) – (e)¹ and, in the case of (f) - (g)², for the purpose of both identity verification and notifying next of kin. I recognise that there are circumstances where it is necessary to be able to verify a person's identity and have knowledge of their marriage or civil union status, however in the case of (a) – (e) identity information alone (i.e. birth or name change information) appears sufficient. Restricting the circumstances under which agencies may access a third party's (such as spouses') information would ensure that this provision is not used arbitrarily and would help protect the privacy rights of those third parties who are not subject to arrest or detention. This amendment would be consistent with the purpose provisions contained in Schedule 1 (new Schedule 4A Privacy Act 1993).

Amendments to Customs and Excise Act

Definition of personal information

19. I **recommend** that a definition of 'personal information' not be included in the Customs and Excise Act but instead be replaced with a cross reference to the definition contained in the Privacy Act. Alternate definitions may cause confusion in regard to application and use and potentially cast doubt over whether the Privacy Act also applies to biometric information.
20. The Privacy Act defines personal information as "information about an identifiable individual; and includes information relating to a death [...]". The proposed definition in clause 14 to be contained in the Customs and Excise Act is "information about an identifiable person (including, without limitation, biometric information)".

¹ That is in the case of a person:

"(a) is, or is liable to be, detained under an enactment:

(b) is, or is liable to be, arrested under a warrant issued by a court or any Registrar:

(c) is contravening, or is about to contravene, an enactment or a court order:

(d) is liable to be prosecuted for an offence punishable by imprisonment:

(e) is, or is liable to be, detained or arrested in respect of a traffic offence"

² That is in the case of a person:

"(f) is endangering, or is threatening to endanger, the life, health, or safety of a person or group of persons:

(g) is injured or dead."

21. The proposed definition in clause 14, while largely consistent with the definition contained in the Privacy Act, includes the further explanation regarding the inclusion of biometric information. This addition appears to suggest that the current definition contained in the Privacy Act does not include biometric information. It is my view that the Privacy Act definition of personal information already includes biometric information; therefore an additional definition is not necessary.

Sharing biometric information with the Police

22. I **recommend** that Police access to Customs' identity information should be granted on a case by case or request basis and not through wholesale direct access or bulk transfer.

23. The border is a unique environment where Customs can use intrusive and coercive powers not normally available to domestic agencies such as the Police. Citizens have the right not to provide information to the Police except under specified circumstances. Allowing Police direct access to information that Customs has the ability to compel from people would circumvent that right.

24. The basis for providing the Police with direct access to biometric information collected by Customs under clause 15, new section 32E, should be carefully assessed. Citizens do not have to provide their fingerprints or other biometric information to the Police unless under arrest. I am therefore in agreement with the Law Society's position contained in its letter to Customs that, "that right should not change just because a citizen has crossed a border. Giving Police direct access to the database would circumvent that right"³.

25. In *Reid v Comptroller of Customs* the court acknowledged the uniqueness of Customs powers. In this case the Judge considered the scope of the powers available to Customs under section 161, which allows the Chief Executive to require a person to produce documents for inspection or to appear before a Customs officer to answer questions:

"the legislature has obviously concluded that the importance of maintaining our border controls and properly and effectively executing the revenue and fiscal implications of the Act are so great as to warrant removal of what is otherwise a common law right".

26. Similarly, in a recent Court of Appeal case (*S v R*) the court noted:

"the power to inspect and examine without warrant may be seen as justified given the often short time available upon the arrival or departure of passengers at busy airports and the difficulty of detecting the importation of prohibited goods. The existence of powers such as those in s 151 may be described as draconian but necessary given the purposes of the legislation and the context in which the powers are exercised".

³ Letter to the New Zealand Customs Service, dated 1 May 2015, titled '*Customs and Excise Act 1996 Review – Discussion Paper 2015*', from the New Zealand Law Society.

27. It is therefore important that restrictions on other agencies' information gathering powers are not unintentionally undermined by the information sharing provisions in this Bill.

Sharing biometric information with overseas agencies

28. Clause 21 amends section 281 and allows Customs to share biometric information with an overseas body. The amendment states that Customs may not share biometric information for the purposes of the overseas agency enforcing a law that imposes a pecuniary (financial) penalty. This potentially means that Customs could share biometric information for all other purposes specified under section 281.

29. The Mutual Assistance in Criminal Matters Act 1992 (MACMA) (Part 3) provides important information sharing considerations for requests made to New Zealand to assist in criminal investigations or proceedings. I consider the MACMA to contain a valuable framework for information sharing internationally.

30. In relation to the sharing of biometrics internationally, I **recommend** that similar protections to those contained in section 27 of MACMA apply to the disclosure of biometrics to an overseas agency by Customs. These protections could include that the Chief Executive must be satisfied that the overseas agency will not use torture or cruel, inhumane or degrading treatment in accordance with the United Nation's Convention Against Torture and that the person will not be subject to capital punishment should prosecution occur, consistent with New Zealand law.

31. This amendment is necessary to ensure that any biometric information shared by Customs is not used in a manner that would violate New Zealand's domestic and international human rights obligations.

Sharing 'personal information' with overseas agencies

32. I **recommend** that clause 22 be removed or amended. Section 282 of the Customs and Excise Act which clause 22 seeks to amend, states what information Customs may share with an overseas agency. Clause 22 proposes to include 'personal information' in the list of information that may be shared.

33. The proposed amendment to include 'personal information' in the list of information that may be disclosed appears to conflict with the specificity found in section 282 presently. This amendment significantly broadens the scope of information Customs could potentially share with an overseas agency and could conceivably include sensitive information such as a person's sexual orientation and political opinions which in a less enlightened jurisdiction could put the subject in grave peril or at risk of discrimination on grounds that would be unlawful in New Zealand.

34. The need for an amendment is not clear, given that section 282 already includes the ability to share “personal identification details (which may include photographs, distinguishing features, and details of identity or travel documents)”. Therefore, if the intent was to allow for the sharing of biometric information, the clause should instead state “(j) biometric information”.

EU privacy adequacy

35. It is important to note the international implications of New Zealand’s domestic legislation relating to Customs, including the privacy dimension. In particular, one consideration is the potential impact on New Zealand’s European Union (EU) adequacy status.

36. New Zealand’s privacy framework has been assessed as being adequate under EU law. In 2012, the European Commission formally ruled that New Zealand’s privacy laws provided adequate personal data protection under European data protection standards. This is significant for New Zealand’s trade relationship as it means that personal information can be sent to New Zealand from Europe without European companies having to take additional measures to ensure the privacy and security of that information. Importantly, adequacy removes the barrier to EU entities transacting business with New Zealand that involves the personal data of EU citizens.

37. Such findings of adequacy are rare and hard-won. Only five⁴ countries outside Europe have obtained this advantage. The Privacy Commissioner provides periodic update reports to the European Commission on developments in New Zealand privacy law⁵. My concern is to ensure that New Zealand’s adequacy finding is not put at risk of re-examination. I therefore echo the Law Commission’s view⁶ that the EU expects New Zealand to protect personal information in accordance with New Zealand’s EU adequacy status. Re-examination could have significant economic and trade impacts for New Zealand.

38. The Court of Justice of the European Union found that data protection authorities could examine complaints that questioned the EU’s data protection adequacy findings. The effect is that in the event of such a complaint, data protection authorities must examine the adequacy status of third countries – such as New Zealand – with ‘all due diligence’⁷.

39. It is therefore vital, given Customs’ international dimension, that they collect, store and use biometric information in accordance with the Privacy Act, which underpins our EU adequacy status. Similarly, it is imperative that legislation governing the sharing of information is not interpreted as overly broad or open-ended with the result that New Zealand’s EU adequacy status be put at risk.

⁴ Argentina, Canada, Israel, and Uruguay.

⁵ <https://privacy.org.nz/blog/update-on-nzs-adequacy-under-the-eu-data-protection-directive/>

⁶ Letter to the New Zealand Customs Service, dated 1 May 2015, ‘*Customs and Excise Act 1996 Review – Discussion Paper 2015*’, from the New Zealand Law Society

⁷ See Brent Tuttle, “*On the adequacy of an adequacy decision post-Schrems*” (1 June 2016) available at: <https://iapp.org/news/a/on-the-adequacy-of-an-adequacy-decision-post-schrems/>

Conclusion

40. Section 21 of the New Zealand Bill of Rights Act 1990 would apply to the information gathering powers and direct access⁸ provisions contained in the Bill. These powers therefore need to be reasonable; this includes that they are necessary, proportionate and have applicable safeguards. Reasonableness tests should also apply to the legislative definitions that underpin the scope of this legislation.
41. In my view, it should be possible to develop appropriate oversight mechanisms for the proposed amendments and provide appropriate clarifications in the final draft. This serves public trust, confidence and accountability.
42. I trust that the recommendations included in this submission will assist the Committee in ensuring this Bill meets both the identity verification needs of agencies included in the Bill and also provides appropriate privacy safeguards and transparency mechanisms.
43. I would be pleased to speak to this submission should the Committee find that helpful in its consideration of this Bill.



Becci Whitton

Team Manager, Policy

for

John Edwards

Privacy Commissioner

⁸ Advice on the consistency of the Intelligence and Security Bill 2016 with the Bill of Rights Act - <https://www.justice.govt.nz/assets/Documents/Publications/nz-intelligence-and-security-bill.pdf>

Appendix A: Summary of Recommendations

Recommendation 1: I recommend that the committee consider whether the Bill should proceed with addition of Part 10A and the associated Schedule in the Privacy Act.

Recommendation 2: I recommend the definition of 'identity information' (clause 6) be limited to the types of information contained in (a)-(e) of that definition.

Recommendation 3: I recommend that clause 6, new section 109E be amended to specifically include a requirement to consult the Privacy Commissioner.

Recommendation 4: I recommend that clause 6, new section 109E be amended by inserting sub clause (3), which would state "the Privacy Commissioner must also be consulted whenever an agreement is substantively amended".

Recommendation 5: I recommend that clause 6, new section 109E mirror the requirements contained in section 95E of the Policing Act 2008.

Recommendation 6: I recommend that clause 12 state that the Registrar-General may share specified personal information with an agency for the purpose of verifying a person's identity in the case of new section 78AB (a)-(e) and, in the case of new section 78AB (f)-(g), for the purpose of both identity verification and notifying next of kin.

Recommendation 7: I recommend that a definition of 'personal information' not be included in the Customs and Excise Act, but instead cross reference the definition contained in the Privacy Act 1993.

Recommendation 8: I recommend that Police access to Customs' identity information should be granted on a case by case or request basis not through wholesale direct access or bulk transfer.

Recommendation 9: I recommend that similar protections to those contained in section 27 of the Mutual Assistance in Criminal Matters Act 1992 also apply to the disclosure of biometrics to an overseas agency by Customs.

Recommendation 10: I recommend that clause 22 be removed or amended to state "(j) biometric information".