Privacy Commissioner
Te Mana Matapono Matatapu

Privacy Commissioner's submission to the Law and Order Committee on the Anti-Money Laundering and Countering Financing of Terrorism Amendment Bill

Executive summary

1. The Anti-Money Laundering and Countering Financing of Terrorism Amendment Bill ("the Bill") amends the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (the AML/CFT Act). Under the expanded AML/CFT regime the core obligations that currently apply to banks, financial institutions, and casinos will also apply to real estate agents, lawyers, accountants, conveyancers, the New Zealand Racing Board, and some high-value dealers.

2. This submission focusses on the provision in the Bill that give new and expanded powers for agencies to share information, including personal information. These provide for the collection and disclosure of the personal information of a significant number of individuals and will therefore have significant implications for personal privacy.

3. My view is that the framework for information sharing provided under clauses 38, 40 and 48 is confusing, contains unnecessary duplication, and gives disproportionate powers to agencies to share information in a way that goes beyond the objectives of the Bill and risks undermining privacy protections in other statutes.

4. In summary, I recommend that the Committee:

   - amend the definition of "law enforcement purposes" in clause 5 to ensure that it cannot be read broadly to include functions outside the purposes of the AML/CFT regime and to ensure that information sharing authorised by officials is appropriately constrained;
   - amend the Bill to create a single regulation making power, with appropriate safeguards, related to information sharing;
   - remove section 139(3)(b) from the Bill;
   - remove section 140A from the Bill and instead require agencies to seek approval for direct access arrangements through Order in Council, either under a regulation making power referred to above or through the approved information sharing agreement mechanism contained in Part 9A of the Privacy Act 1993; and
   - ensure concerns identified in the Privacy Impact Assessment conducted for this Bill are addressed before the Bill progresses.

Background

5. I support the objective of the proposed changes to the AML/CFT regime which aim to strike a balance between combating crime, minimising costs and enabling New Zealand to meet its international obligations under the Financial Action Taskforce and to engage in international efforts to detect and deter money laundering and terrorism financing to detect and deter money laundering and terrorism financing.

6. I also supported the recommendations of the *Government Inquiry into Foreign Trust Disclosure Rules* (the Shewan Report) as I acknowledge the importance of a robust AML/CFT regime that provides appropriately for the information sharing needed to meet both our domestic interests and international cooperation objectives. One of the stated aims of the Bill is to implement recommendations from that Report by providing greater flexibility to share information to meet the purposes of the Act.

7. I was pleased to have the opportunity to comment on an Exposure Draft of the Bill, and note that the Bill includes some changes that reflect the comments I made during that consultation. However, substantive changes have been made to the information sharing provisions which means that, compared to the Exposure Draft, I no longer view them as proportionate nor the safeguards as adequate.

8. I consider the information sharing regime provided for under the Bill as currently drafted is ill-defined, overly broad and goes well beyond what is necessary to give effect to the Shewan Report's recommendations or to provide for an effective and efficient AML/CFT regime.

9. The Departmental Disclosure statement accompanying the Bill advised that a preliminary Privacy Impact Assessment (PIA) has been completed, but it did not clarify the nature of additional safeguards deemed necessary to ensure the revised legislation will not unduly impact on the privacy of individuals. If that privacy analysis identified the need for specific mitigations to address privacy risks, I **recommend** that these be addressed before the Bill progresses.

Information sharing provisions are disproportionate, confusing, and do not include adequate safeguards

10. The information sharing provisions in clauses 38, 40 and 48 go beyond what is necessary to give effect to the recommendations of the Shewan Report, and would give disproportionate powers to officials to share personal information. They are also confusing, giving multiple mechanisms under which information sharing can occur, with some mechanisms containing considerably fewer safeguards than others, without apparent justification.

11. As discussed below, these information sharing powers should be more tightly constrained to the purposes of the AML/CFT regime, simplified, and stronger safeguards included.

The purposes for which officials are permitted to share personal information, without oversight, should be clearly defined and limited

12. Clause 38 replaces section 139. New sections 139(1) and (2) expand the existing information sharing powers such that the Commissioner, the New Zealand Customs Service, or an AML/CFT supervisor may disclose any information (the current Act explicitly excludes personal information) to any other government agency or regulator for "law enforcement purposes" or "regulatory purposes".

13. The definition of "law enforcement purposes" in the Bill is very broad. It expands the current definition, meaning the new sections 139(1) and (2) give officials a disproportionate power to share personal information with a very wide range of agencies.

14. The current Act defines "law enforcement purposes" as the administration of this Act, the detection, investigation and prosecution of offences under the Act and money laundering offences, the enforcement of a list of related statues, and actions taken in respect of legislation of overseas jurisdictions that are broadly equivalent to the enactments listed. Clause 5 of the Bill expands the definition of "law enforcement purposes" to include:

    - "intelligence gathering and analysis"; and
    - "national security and defence".

15. The expanded definition is problematic. The lack of specificity, for example, of a term such as "national security and defence", combined with the broad powers for officials to share information, create the risk of inappropriate information disclosure outside of the purposes of the AML/CFT regime.

16. Legislative authority for officials to share personal information, without oversight by Ministers or Parliament, is only appropriate where the purposes for disclosure are clearly defined and limited. I therefore **recommend** that the definition of "law enforcement purposes" in the Bill be refined to ensure that it is clearly restricted to activities related to the AML/CFT regime, and cannot be read inappropriately broadly.

17. If the intention is to allow officials to share information for broad purposes, then I **recommend** that additional safeguards included, such as that information sharing arrangements can only be approved by Order in Council following consultation with the Privacy Commissioner.

The circumstances in which the Bill requires regulations to authorise information sharing should be clarified

18. The Bill also creates two avenues for agencies to seek regulations to permit information sharing beyond that permitted in new sections 139(1) and (2). These provisions are confusing, and it is not clear why two regulation making powers are required or in what circumstances agencies would need to seek regulations rather than relying on the information sharing powers in sections 139(1) and (2).

19. New section 139(3)(a) provides that where not authorised by sections 139(1) and (2), disclosures of information between agencies for law enforcement or regulatory purposes may be authorised by regulations made under sections 139A or 153.

20. The new regulation making powers in section 139A, inserted by clause 38, allow for regulations to be approved by Order in Council that allow agencies to share information. This is limited, due to section 139(3), to sharing for law enforcement or regulatory purposes, and includes the safeguard of consultation with the Privacy Commissioner before regulations are finalised (section 139A(2)(b)).

21. Section 153 in the current Act allows regulations to be made by Order in Council for a range of purposes. Clause 48 of the Bill amends this section to add new purposes for which regulations can be made, including: sections 153(ia), "authorising and regulating the sharing of information between reporting entities in different groups"; and, (ib), "authorising and regulating the sharing of information between the Commissioner, the New Zealand Customs Service, AML/CFT supervisors, and international authorities".

22. Section 139(3) means that the new sections 153(ia) and (ib) include personal information, and restricts the purposes for sharing to law enforcement and regulatory purposes. However, in contrast to new section 139A, no consultation requirements apply before regulations are finalised under section 153. This is particularly problematic considering new section 153(ib) includes international information sharing. By allowing multiple avenues for sharing information, there is a risk that the Bill creates a situation where officials will seek the least resource intensive path, rather than the option with the most appropriate safeguards.

23. I **recommended** that the Bill be revised to create a single regulation making provision to provide for the information sharing required for the effective administration of the AML/CFT regime, including sharing with overseas agencies. This regulation making power should include appropriate safeguards, including specification of the information that can be shared, a requirement for consultation with the Privacy Commissioner before regulations are finalised, and provision for information sharing arrangements to be periodically reviewed.

The authority for officials to enter into written agreements allowing for information sharing should be removed from the Bill

24. New section 139(3)(b), states that in the absence of regulations, information sharing can be authorised by a written agreement between agencies.[1] Why section 139(3)(b) is required is not clear, given the ability to share information under sections 139(1) and (2).

25. This section would appear to create an avenue for officials to avoid the requirement to seek regulations under sections 139A or 153, thus bypassing any Ministerial or Parliamentary oversight. I therefore **recommend** that new section 139(3)(b) be removed from the Bill.

[1] Written agreements must contain the information set out in new section 140A(3) (inserted by clause 40).

The power for officials to enter into written agreements allowing for direct access to agencies' databases should be removed from the Bill

26. Clause 40 inserts new section 140A, that creates a power for officials to enter into written agreements to "facilitate access to data holdings" for law enforcement purposes. New section 140A(2) allows officials to agree, by written agreement, to disclose "any relevant information" between government agencies, to allow direct access to government agencies' databases, and to disclose "any relevant information" to international counterparts in accordance with regulations (the wording of new section 139(3) means that this would include personal information).

27. Allowing direct access to databases is appropriate in some exceptional circumstances. For example, the Intelligence and Security Act 2017[2] allows intelligence and security agencies, due to the exceptional nature of their work, to have direct access to information held by other agencies, in accordance with written agreements between Ministers. The Enhancing Identity Verification and Border Processes Legislation Bill[3] (currently awaiting its second reading), would allow agencies listed in a schedule to have direct access to certain limited types of information for identity verification purposes.

28. In contrast, the power to enter into direct access agreements created by new section 140A applies neither to agencies whose work is exceptional, nor is the purpose or type of information that can be accessed appropriately constrained. There is a risk that if it proceeds as currently drafted, new section 140A could undermine controls on access to information by the intelligence and security agencies that Parliament has recently enacted as well as those contained in statutes governing the New Zealand Police, Inland Revenue and the New Zealand Customs Service.

29. It is not clear why such a broad power to allow direct access is required for the purposes of the AML/CFT regime, nor why the power to enter into written agreements should be delegated to officials rather than being approved by Order in Council. No other public sector chief executives have the authority to enter into agreements that override people's privacy rights in this way. I note that all government agencies have access to the approved information sharing agreement mechanism contained in Part 9A of the Privacy Act 1993. This mechanism can be used to authorise direct access arrangements and includes appropriate safeguards.

30. I **recommend** that section 140A be removed from the Bill. A regulation making power, referred to above, or the existing approved information sharing agreement contained in Part 9A of the Privacy Act, would both be more appropriate mechanisms for authorising direct access to databases, if this is required for the effective administration of the AML/CFT regime.

---

[2] Section 125.

[3] Section 109E inserted by clause 6.

Conclusion

31. I trust the recommendations included in this submission will assist the Committee in ensuring this Bill meets the needs of agencies operating under the AML/CFT regime in a proportionate manner.

32. I request to speak to the Committee regarding this submission.

John Edwards
Privacy Commissioner