Australian Government

Office of the Australian Information Commissioner

Inquiry into the provisions of the Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

28 January 2020

OAIC

January 2020

Contents

Executive Summary 2

Ensuring that all individuals who are permitted to access, use and disclose AUSTRAC information are subject to privacy safeguards 3

Disclosure of AUSTRAC information overseas 4

Executive Summary

1. The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to provide a submission to the Senate Legal and Constitutional Affairs Legislation Committee in relation to the inquiry into the provisions of the Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019 (the Bill).
2. The Bill amends the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) to, amongst other things, expand the exceptions to the prohibition on tipping off to permit reporting entities to share suspicious matter reports (SMRs) and related information with external auditors, foreign members of corporate groups and designated business groups.
3. The current list of 'designated agencies' is repealed and replaced by a broader definition of 'Commonwealth, State and Territory agency', which specifies categories of agencies rather than individual agencies who may be authorised to access, use and disclose AUSTRAC information.
4. The Bill also expands the information sharing powers of the Chief Executive Officer (CEO) of the Australian Transaction Reports and Analysis Centre (AUSTRAC) including to:
    - allow the AUSTRAC CEO to:
        a. authorise 'specified officials' of Commonwealth, State or Territory agencies to access AUSTRAC information;
        b. impose conditions on certain persons who have received AUSTRAC information
    - provide for an AUSTRAC official to disclose AUSTRAC information to a Minister for performance of their responsibilities; and
    - provide for a member of a taskforce established by the AUSTRAC CEO to deal with AUSTRAC information in the same way an AUSTRAC official can deal with AUSTRAC information.
5. The OAIC acknowledges the important public policy objectives of the Bill to strengthen Australia's capabilities to address money laundering and terrorism financing risks. These amendments respond to recommendations in the 2016 *Report on the Statutory Review of the AML/CTF Act and associated Rules and Regulations*, including by expanding the permissible uses of AUSTRAC information and facilitating effective and efficient information sharing between domestic and international partner agencies.[1]
6. The Bill expands the circumstances in which 'AUSTRAC information' may be collected, used and disclosed. Where AUSTRAC information reasonably identifies an individual it is 'personal information' for the purposes of the *Privacy Act 1988* (Cth) (Privacy Act). The Explanatory Memorandum states AUSTRAC information can be 'highly personal and sensitive'.[2] AUSTRAC's privacy statement[3] references the Privacy Act, noting that it collects information, including 'sensitive information'. This may include information about an individuals' criminal record, race

[1] *Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations* (2016) <https://www.homeaffairs.gov.au/help-and-support/how-to-engage-us/consultations/statutory-review-of-the-anti-money-laundering-and-counter-terrorism-financing-act-2006>.

[2] Explanatory Memorandum, Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019, page 35, paragraph 201.

[3] https://www.austrac.gov.au/privacy/austrac-privacy-statement

or ethnicity, religious beliefs or affiliations, biometric information, health information and sexual orientation or practices.[4]

7. While Australia's privacy laws recognise that the protection of individuals' privacy is not an absolute right, any impact on privacy must be subject to a careful assessment of its necessity, legitimacy and proportionality.[5] For law enforcement initiatives that adversely impact privacy, this includes demonstrating the necessity of the proposal and ensuring that the scope of proposed measures is proportionate and transparent.

8. Where an adverse impact on privacy is necessary, a commensurate increase in oversight, accountability and transparency should be considered in order to strike an appropriate balance between any privacy impacts and law enforcement and national security objectives.

9. A Privacy Impact Assessment (PIA) would assist in considering these matters. A PIA can identify privacy impacts of a Bill, and set out recommendations for managing, minimising or eliminating those impacts. A PIA would also inform the Explanatory Memorandum, including the Statement of Compatibility with Human Rights.[6]

10. The Australian Government Agencies Privacy Code requires Government agencies to conduct a PIA for all high privacy risk projects, which includes any new or changed ways of handling personal information that is likely to have a significant impact on the privacy of individuals.

11. The Australian Information Commissioner and Privacy Commissioner (the Commissioner) has statutory monitoring related functions under the Privacy Act. The OAIC provides this submission, including two recommendations, which are aimed at ensuring appropriate safeguards are in place to mitigate against any adverse effects on the privacy of Australians, pursuant to paragraph 28A(2)(c) of the Privacy Act.

Ensuring that all individuals who are permitted to access, use and disclose AUSTRAC information are subject to privacy safeguards

12. It is important that AUSTRAC information being shared across the domestic law enforcement community is subject to consistent, comprehensive privacy protections. The Bill proposes the use and disclosure of AUSTRAC information to additional organisations not currently contemplated by the existing legislation. While some of those organisations are currently required to comply with the Commonwealth Privacy Act, others are not. To the extent that the additional organisations are not reporting entities or otherwise subject to the Privacy Act, the OAIC recommends that they are brought within the jurisdiction of that Act to ensure consistent and adequate privacy protections across all parts of the ecosystem.

---

[4] *Privacy Act 1988* (Cth), section 6(1).

[5] See Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age UN Doc A/HRC/27/37 (2014), paragraph 23, <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx>.

[6] The OAIC has published a Guide to undertaking privacy impact assessments <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/>, as well as a Privacy Impact Assessment e-learning tool <https://www.oaic.gov.au/s/elearning/pia/>.

13. Organisations not currently within the jurisdiction of the Commonwealth Privacy Act may include individuals engaged to conduct an audit or review[7], members of a taskforce[8] and State and Territory agencies.

14. State and Territory agencies may currently access AUSTRAC information following the provision of an undertaking to comply with particularised privacy protections. However, since the inception of this law, there have been additional privacy safeguards introduced into the Commonwealth Privacy Act, including the Notifiable Data Breaches (NDB) scheme. The NDB scheme requires organisations to assess whether or not a data breach is likely to cause significant harm to those whose personal information has been compromised as a result of the breach, and provide notifications to the Information Commissioner and the affected individuals in the event that threshold is met.

15. Requiring State and Territory agencies to be brought within the jurisdiction of the Commonwealth Privacy Act to the extent that they deal with AUSTRAC information would ensure that there are consistent privacy protections regardless of the nature of the organisation dealing with the information. Section 6F of the Privacy Act allows a State or Territory agency to be prescribed as an 'organisation' in relation to specific acts or practices — such as in relation to AUSTRAC information. This would assist in providing an enhanced and consistent level of privacy protection in relation to AUSTRAC information that is handled within Australia, noting that any currently exempted bodies such as intelligence agencies and exceptions in relation to 'enforcement' bodies and 'enforcement related activity' would not be affected.[9]

Recommendation 1

The OAIC recommends that all individuals and entities who are permitted to access, use or disclose AUSTRAC information are covered by the Commonwealth Privacy Act to the extent that they deal with that information.

Disclosure of AUSTRAC information overseas

16. Where AUSTRAC information is disclosed overseas, it is important that privacy safeguards are in place to protect the personal information of Australians and mitigate against privacy risks.

17. One such privacy safeguard is an undertaking provided by a foreign recipient of AUSTRAC information to protect the confidentiality and control the use of the information and ensure that information will only be used for the purpose for which it is disclosed.

[7] See subclause 123(5B) of the Bill.

[8] See paragraph 212(1(da) and item 39 of the Bill.

[9] See section 7 of the Privacy Act in relation to acts or practices of intelligence agencies which are exempt. See also the definition of 'enforcement body' and 'enforcement related activity' in section 6(1) of the Privacy Act, which includes State and Territory agencies.

18. The current law requires undertakings to be obtained by the AUSTRAC CEO and certain Commonwealth agencies prior to disclosing AUSTRAC information overseas.[10] The Bill further relies on undertakings as a privacy safeguard in relation to disclosures of AUSTRAC information to overseas members of corporate groups and designated business groups.

19. Subclause 127(1) of the Bill proposes to amend section 132, making it discretionary, rather than mandatory, for the AUSTRAC CEO to seek an undertaking from an overseas government prior to disclosing AUSTRAC information overseas.

20. The Explanatory Memorandum states that this amendment is to allow for 'effective disclosure of less sensitive AUSTRAC information in international forums attended by AUSTRAC and international presentations/workshops given by AUSTRAC, for example during capacity building exercises for regional partners.'[11]

21. There are differences between the use of AUSTRAC information for the purposes of capacity building with international partners, and for the purpose of monitoring an Australian suspected of money-laundering and terrorism financing activities.

22. Where AUSTRAC information containing personal information is disclosed in an international forum, the information should be appropriately de-identified. If information is de-identified, then the Privacy Act will not apply. However, where the information identifies an individual, or is about an individual that is reasonably identifiable, safeguards must be in place to mitigate against the potential privacy impacts which could arise through disclosure.

23. The proposed amendment to the current section 132(1) may be unnecessary to give effect to the stated policy intention, noting that the information should be appropriately de-identified prior to being disclosed internationally for a secondary purpose. Where disclosure of AUSTRAC information that includes personal information is required for capacity-building purposes, it remains appropriate that an undertaking from all overseas participants be obtained.

24. Given the potentially sensitive nature of AUSTRAC information and the privacy risks which may arise when this information is disclosed to a foreign government, the OAIC recommends that the requirement for the AUSTRAC CEO to obtain an undertaking prior to disclosure be retained in the legislation. This would assist in mitigating privacy risks, noting that the requirements in APP 8 that generally apply to APP entities disclosing personal information overseas, are displaced where the disclosure is authorised by another law.

Recommendation 2

The OAIC recommends that the requirement for the AUSTRAC CEO to obtain an undertaking prior to disclosing AUSTRAC information to an overseas government or agency be retained.

[10] See sections 132 – 133C of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006.*

[11] Explanatory Memorandum, Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019, page 36, paragraph 213.

25. The OAIC has published guidance which entities may find useful in considering the nature and content of the undertakings which are utilised to protect AUSTRAC information.[12] The OAIC's resources may also assist more generally in relation to protecting personal information.

26. Furthermore, the Commissioner is available to provide advice and guidance to the AUSTRAC CEO in relation to privacy functions, in accordance with section 212(2)(a)(vi) of the AML/CTF Act.

27. The OAIC is available to provide further assistance to the Committee as required.

[12] See, for example, the Australian Privacy Principle Guidelines <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/>, the Guide to Undertaking Privacy Impact Assessments < https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/> and 'De-identification and the Privacy Act <https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/>.