Australian Government
Department of Home Affairs

Senate Legal & Constitutional Affairs Legislation Committee: Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019

Department of Home Affairs and AUSTRAC joint responses to Questions on Notice.

Index

HOME AFFAIRS PORTFOLIO

DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Legal and Constitutional Affairs Legislation Committee

14 February 2020

QoN Number: AMLCTF/001

Subject: Recommendations from the Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and associated rules and regulations

Asked by: Senator Amanda Stoker

Question:

How has the department addressed the recommendations from the Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and associated rules and regulations?

Answer:

This is still in progress. The Australian Government is taking a phased approach to reforming the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) regime that prevents criminals from enjoying the profits of their illegal activities, and stops funds falling into the hands of terrorists.

In 2017, the Government addressed 17 recommendations (whilst also addressing 3 recommendations partially) from the Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and associated rules and regulations (the Statutory Review Report). The 2017 reforms amended the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the AML/CTF Act) to regulate digital currency exchange providers and expand the supervisory and enforcement options available to Australia's AML/CTF regulator, the Australian Transaction Reports and Analysis Centre (AUSTRAC).

The Anti-Money Laundering and Other Legislation Amendment Bill 2019 (the Bill) is the second phase of the Government's reforms. The Bill aims to address the following recommendations from the Statutory Review Report:

- simplifying and streamlining the corresponding banking obligations in the AML/CTF regime (R 10.3(a))
- prohibiting financial institutions from forming correspondent banking relationships involving shell banks (R 10.3(c))
- expanding the exemptions to the prohibition on 'tipping-off' (R 14.1)

- consolidating the reporting requirements for currency and bearer negotiable instruments into a single ‘monetary instruments’ reporting scheme (R 12.1), and
- increasing civil penalties for non-compliance with the cross-border movement reporting obligations (R 12.5).

HOME AFFAIRS PORTFOLIO

DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Legal and Constitutional Affairs Legislation Committee

14 February 2020

QoN Number: AMLCTF/002

Subject: How the measures in the bill will improve Australia's compliance with international standards

Asked by: Senator Amanda Stoker

Question:

How will the measures in this bill improve Australia's compliance with the international standards for combating money laundering and terrorism financing set by the Financial Action Task Force? Are there additional measures required to ensure practices in Australia align with international best practice?

Answer:

The Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019 (the Bill) includes reforms relevant to the following Financial Action Task Force (FATF) Recommendations:

- **FATF Recommendation 10 (customer due diligence)**: The Bill would amend section 32 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) to make more explicit the prohibition against a reporting entity providing a designated service where the reporting entity cannot undertake the necessary customer due diligence (CDD). The proposed note to section 32 also highlights the link to section 41 (the obligation to submit a suspicious matter report (SMR)) which could be triggered where a reporting entity cannot carry out the necessary customer due diligence.
- **FATF Recommendation 17 (reliance on third parties)**: The Bill would amend section 38 of the AML/CTF Act to allow reporting entities to rely on other regulated businesses and makes clear the obligation that such reliance must be reasonable having regard to the money laundering and terrorism financing risk. The rule-making power in section 38 would permit other elements of FATF Recommendation 17 to be addressed through enforceable rules made by the AUSTRAC Chief Executive Officer.
- **FATF Recommendation 13 (correspondent banking)**: The proposed new sections 95 and 96 would address the limitations in Australia’s current implementation of FATF Recommendation 13:

- Section 95 would extend the existing prohibition against financial institutions entering correspondent banking relationships with shell banks, or financial institutions that have relationships with shell banks, to prohibit the entering of correspondent banking relationships with financial institutions that *permit* their accounts to be used by shell banks.
- Section 96 would make it mandatory for banks to undertake due diligence assessments before entering *any* correspondent banking relationship, and periodically throughout the course of the relationship. Currently banks are only required to carry out due diligence assessments where they consider one is warranted following a preliminary risk assessment.
- Subsection 96(2) would introduce a timeframe within which a financial institution that has a correspondent banking relationship with another financial institution that involves a vostro account must prepare a written record setting out the responsibilities of both parties. The amendment requires a written record to be prepared within 20 business days of the financial institution entering into the relationship. This subsection implements the requirement under FATF Recommendation 13 for a financial institution to clearly understand the respective responsibilities of each institution in a correspondent banking relationship.

- **FATF Recommendation 18 (internal controls and foreign branches and subsidiaries)**: The amendments to section 123 would expand the exception to the prohibition against "tipping off" when a reporting entity has reported a suspicious matter report to AUSTRAC:
  - The new subsections 123(7), 123(7A), 123(7AA) and 123(7AB) reflect a need to allow reporting entities, and related entities that are part of their global structures, to more effectively manage the risks associated with the international footprint of their business at the group level. Specifically, entities will be able to manage the risk posed by particular customers, noting that some reporting entities already regularly receive suspicious matter reports and related information from foreign-related entities but are unable to reciprocate the disclosure.
  - The new subsection 123(5A) would allow a reporting entity to share a suspicious matter report and related information to external auditors that are auditing or reviewing the reporting entity's AML/CTF program. This further facilitates appropriate risk management and internal controls by reporting entities in line with FATF Recommendation 18.
- **FATF Recommendation 32 (cash couriers)**: The amendments to Part 4 of the AML/CTF Act would implement a new requirement to declare monetary instruments with a value equivalent to AUD 10,000 or more when they are brought or sent into, or taken or sent out of, Australia. This would replace the existing disclosure-on-request framework for bearer negotiable instruments. This is consistent with FATF Recommendation 32 that deals with cash couriers and requires countries to have measures in place to detect the physical cross-border transportation of currency and bearer negotiable

instruments. Amendments to section 186A will increase the civil penalties for failing to declare cross-border movements of physical currency or monetary instruments, in line with FATF Recommendation 32.

- Other amendments may also indirectly strengthen Australia's compliance with the FATF Recommendations. For example, by simplifying the secrecy and access provisions of Part 11 of the AML/CTF Act, AUSTRAC will be better able to disseminate information and analysis to relevant authorities in appropriate circumstances, in line with FATF Recommendation 29 (financial intelligence units).

HOME AFFAIRS PORTFOLIO

DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Legal and Constitutional Affairs Legislation Committee

14 February 2020

QoN Number: AMLCTF/003

Subject: Sectors and services that are required to report to AUSTRAC

Asked by: Senator Amanda Stoker

Question:

Can the Department detail the sectors and services that are required to report to AUSTRAC? How do Australia's reporting requirements compare internationally?

Answer:

Businesses that provide one or more designated service as prescribed in Tables 1 to 3 in section 6 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) are regulated for anti-money laundering and counter-terrorism financing (AML/CTF) purposes. Designated services include a range of business activities in the financial services, remittance, bullion, gambling and digital currency exchange sectors.

Regulated businesses (referred to as 'reporting entities') have the following reporting obligations:

- suspicious matters;
- threshold transaction;
- international funds transfer instructions, and
- compliance.

International comparisons

The Financial Action Task Force (FATF) international standards require all FATF members to implement a suspicious matter reporting requirement as part of their AML/CTF regime. The international funds transfer instruction and threshold transaction reporting obligations under Australia's AML/CTF regime are not required by the FATF standards, but many countries have chosen to impose similar reporting requirements as additional measures to collect enhanced financial intelligence.
For example, New Zealand, Canada and the United States impose a reporting requirement for large cash transactions. The reporting of international funds transfer instructions is required under the New Zealand and Canadian AML/CTF regimes at varying thresholds.

HOME AFFAIRS PORTFOLIO

DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Legal and Constitutional Affairs Legislation Committee

14 February 2020

QoN Number: AMLCTF/004

Subject: Privacy concerns regarding the AMLCTF Bill

Asked by: Senator Amanda Stoker

Question:

Have there been any privacy concerns raised with the department about the bill?

Answer:

The Department of Home Affairs and the Australian Transaction Reports and Analysis Centre (AUSTRAC) conducted an extensive consultation process with peak industry bodies and Commonwealth, State and Territory agencies during the development of the Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019 (the Bill).

On 17 December 2018, the Department provided relevant stakeholders with an exposure draft of Part 4 of the Bill, which deals with the use and disclosure of AUSTRAC information. Privacy concerns raised by stakeholders during this consultation process were considered by the Department, and addressed accordingly in subsequent iterations of the Bill.

The Department also sought the advice of the Australian Government Solicitor on the privacy implications of the Bill. Please see the **attachment A** Privacy Impact Assessment (PIA). The PIA has been used to inform the Explanatory Memorandum of the Bill, including the Statement of Compatibility with Human Rights.

Australian Government Solicitor
4 National Circuit Barton ACT 2600
Locked Bag 7246 Canberra Mail Centre ACT 2610
T 02 6253 7000 DX 5678 Canberra
www.ags.gov.au

Canberra
Sydney
Melbourne
Brisbane
Perth
Adelaide
Hobart
Darwin

REPORT

PRIVACY IMPACT ASSESSMENT: DRAFT *ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING AND OTHER LEGISLATION AMENDMENT BILL 2019*

25 February 2019

To:
Anti-Money Laundering & Counter-Terrorism Financing Reform Section
Transnational Crime Policy Branch
National Security and Law Enforcement Policy Division
Department of Home Affairs
3-5 National Circuit
BARTON ACT 2600

File reference: 18009202

REPORT

PRIVACY IMPACT ASSESSMENT: DRAFT *ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING AND OTHER LEGISLATION AMENDMENT BILL 2019*

1. The Department of Home Affairs (the Department) has asked us to conduct a privacy impact assessment (PIA) in relation to the following provisions in the draft *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2019* (the draft Bill):

   - the secrecy and access provisions
   - the tipping off offence provisions.

2. Australian Privacy Principle (APP) 1.2 in Schedule 1 to the *Privacy Act 1988* (the Privacy Act) requires that agencies such as the Department take reasonable steps to implement practices, procedures and systems that will ensure compliance with the APPs and will enable the Department to deal with enquiries and complaints about compliance with the APPs. This PIA is a key part of the activities undertaken by the Department to identify possible privacy impacts from the draft Bill. This report recommends potential solutions that the Department might implement to minimise or eliminate those privacy impacts.

SUMMARY OF FINDINGS

3. The flow of personal information under the amendments proposed to be introduced by the draft Bill has been assessed for compliance with the requirements of the Privacy Act and the APPs.

4. Based on our assessment of potential privacy impacts set out in Part 3 of this PIA, we consider that, while the proposed amendments will raise a number of potential privacy implications, these can be mitigated appropriately by the Department and / or other relevant Commonwealth agencies, or managed consistently with the APPs.

HOW IS THIS PIA STRUCTURED?

5. This PIA is divided into the following sections:

   - Part 1: The **introduction** section outlines the information provided to us by the Department and the material we have reviewed, sets out the scope and contextual background of this PIA and notes the assumptions we have made in preparing this PIA.
   - Part 2: The **focus of this PIA** section describes what the relevant portions of the draft Bill will do.
   - Part 3: The **privacy impact analysis – privacy implications and analysis of personal information flows** section examines the changes that will be made by the draft Bill from a privacy perspective, by identifying and examining relevant data flows (including data that comprises personal information) and analysing the effect and impact of these changes having regard to the existing

and ongoing privacy obligations of the various entities that will be affected by these changes.

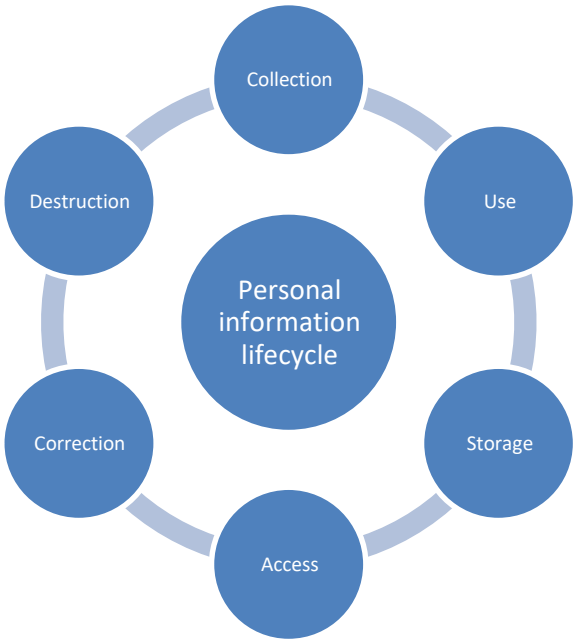
These sections are followed by **a summary of our views on the overall effect and impact of these changes and related recommendations** on the various matters discussed in this PIA.

PART 1: INTRODUCTION

Why is the Privacy Act relevant here?

6. The APPs detail how personal information must be handled over the life cycle of the information. This includes how personal information should be collected, stored, used, disclosed, accessed, corrected and destroyed. The APPs also impose higher protections for personal information which falls within the definition of sensitive information.

7. Additionally, from 1 July 2018, all agencies subject to the Privacy Act are also bound by the Australian Government Agencies Privacy Code (Privacy Code).[1] The Code sets out specific requirements that agencies must meet to comply with APP 1.2, including the conduct of a PIA for all 'high risk' projects: see s 12(1).[2]



8. A PIA examines the lifecycle of personal information handled by a system or project or through the operation of legislative provisions to identify any potential or actual privacy issues. The final PIA report will identify concerns and make recommendations on how to mitigate or remove any privacy issues. Where an agency subsequently implements the recommended practices, this will enable compliance with APP 1.2.

---

1 The *Privacy (Australian Government Agencies — Governance) APP Code 2017* is available at: https://www.legislation.gov.au/Details/F2017L01396. Section 26A of the Privacy Act requires an entity not to do an act, or engage in a practice, that breaches a registered APP code that binds the entity. An APP Code may set out how an APP is to be complied with: s 26C(2)(a).

2 A 'high risk project' is defined in s 12(2) of the Privacy Code to be any project involving any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

Information provided and material reviewed

9. This PIA has been prepared having regard to:

- the Department's instructions to AGS
- the Department's drafting instructions to the Office of Parliamentary Counsel
- relevant extracts from the *Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations* (the Statutory Review Report).[3]

10. This PIA is based on the secrecy and access provisions and tipping off offence provisions as set out in Schedule 1 to the version of the draft Bill dated 25 January 2019.[4]

11. More broadly, we have examined and considered the relevant operation of the Privacy Act and those parts of the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (the AML/CTF Act) that are proposed to be amended by the draft Bill. We have also referred to the *Guide to undertaking privacy impact assessments*[5] issued by the Office of the Australian Information Commissioner (OAIC) in May 2014 and the OAIC's *APP guidelines*.[6]

Assumptions made

12. This PIA has been prepared on the assumption that the AML/CTF Act is amended as is currently proposed by the above provisions set out the draft Bill. For this reason, the comments made and the conclusions reached should be taken to apply only to the amendments as reflected in the version of the draft Bill provisions considered in this PIA.

13. This PIA also assumes that the agency employees and other persons subject to the secrecy, access and tipping off obligations under the AML/CTF Act, if amended as proposed, are otherwise aware of, and comply with, the privacy, secrecy and confidentiality obligations that currently apply to their day-to-day handling of information and documents, including personal information.

PART 2: FOCUS OF THIS PIA

14. This PIA relates only to the substantive changes to current Commonwealth legislation that are proposed to be made by the draft Bill. We have identified a variety of relevant changes in this context, which are each described in summary below. For the reasons set out below, we have specifically considered the effect of the proposed amendments with respect to the acts and practices of the Australian Transaction Reports and Analysis Centre (AUSTRAC), the Australian Crime

---

3 Available at: https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/report-on-the-statutory-review-of-the-anti-money-laundering.pdf.

4 B18JC548.v28.docx 25/1/2019 11:24 AM

5 Available at: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.

6 Available at: https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/.

Commission (ACC),[7] the intelligence agencies and the other Commonwealth agencies that deal with those agencies, as this aspect raises specific considerations in terms of the scope, operation and relevance of the Privacy Act (and the APPs in particular).

15. In the main, the changes under the draft Bill alter (through consolidation, clarification or expansion) existing information-handling arrangements and obligations under the AML/CTF Act. This PIA does not consider those underlying arrangements and obligations in their totality—we focus only on the novel elements introduced by the draft Bill.

16. Although the proposed changes the draft Bill implements would impose certain information-handling obligations on Commonwealth as well as State and Territory agencies and private sector organisations, this PIA considers only those organisations and Commonwealth agencies. None of the various State and Territory agencies to which AUSTRAC information would be disclosed under the provisions in the Bill are covered by the Privacy Act. We do not consider the potential application of any State or Territory privacy legislation to those agencies in this PIA.

General application of Privacy Act to Commonwealth agencies

17. The secrecy and access amendments proposed to be introduced by the draft Bill are most relevant to the Privacy Act obligations, and general privacy practices, of Commonwealth agencies.

18. AUSTRAC is an 'agency' and 'APP entity' for the purposes of the Privacy Act.

19. Each of the Commonwealth agencies specifically named in proposed new s 127(2) is also an 'agency' and 'APP entity' for the purposes of the Privacy Act, as are the Commonwealth agencies falling within the proposed new definition of 'Commonwealth, State or Territory agency'.

General application of Privacy Act to private sector organisations

20. The tipping off offence amendments proposed to be introduced by the draft Bill are most relevant to the Privacy Act obligations, and general privacy practices, of private sector organisations.

21. The Privacy Act also imposes obligations on certain private-sector 'organisations', defined in s 6C. Relevantly for present purposes, reporting entities within the meaning of s 5 of the AML/CTF Act[8] (including banks, building societies and credit unions), are organisations subject to the Privacy Act.

---

7 'ACC' is used throughout this PIA, given its usage in current Commonwealth legislation. We note, however, that the ACC is now more commonly referred to as the Australian Criminal Intelligence Commission or the ACIC.

8 As persons who provide designated services within s 6 of the AML/CTF Act.

Modified operation of Privacy Act with respect to the activities and records of AUSTRAC, the ACC and intelligence agencies

22. However the Privacy Act has a modified operation in relation to:

- the activities of AUSTRAC
- the activities of the various intelligence agencies which are listed in proposed s 127(2)[9]
- the activities of the ACC
- the dealings of other Commonwealth agencies with these intelligence agencies and the records of these agencies.

23. To the extent that the provisions in the draft Bill may involve:

a. certain acts and practices of AUSTRAC in handling personal information

b. the acts and practices of ASIO, ASIS, ASD, ONI or the ACC in handling personal information

c. certain acts and practices of AGO and DIO in handling personal information

d. an APP entity disclosing personal information held in its records to ASIO, ASIS or ASD

e. an APP entity handling personal information in records originating with or received from ASIO, ASIS, ASD, ONI, AGO, DIO and the ACC

such acts and practices will not be subject to the requirements set out in the APPs.

24. This is due to the operation of various provisions in s 7 the Privacy Act, the effect of which is summarised briefly below.[10]

AUSTRAC

25. Section 7(1)(a)(i) provides that a reference in the Privacy Act to an 'act or practice' engaged in by a body does not include an 'act or practice' engaged in by an agency specified in Division 1 of Part II of Schedule 2 to the *Freedom of Information Act*

---

9 These are: the Australian Crime Commission (ACC), the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Australian Signals Directorate (ASD), the part of the Department of Defence (Defence) known as the Australian Geospatial Intelligence Organisation including any part of the Defence Force that performs functions on behalf of that part of the Department (AGO), the part of Defence known as the Defence Intelligence Organisation including any part of the Defence Force that performs functions on behalf of that part of Defence (DIO) and the Office of National Intelligence (ONI).

10 For completeness, proposed new s 127(2) also refers to other Commonwealth agencies whose acts and practices are not modified by s 7 of the Privacy Act, namely the Department, the Department of Foreign Affairs and Trade, the Attorney-General's Department, the Australian Federal Police (AFP), the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and the Australian Taxation Office.

1982 (FOI Act). AUSTRAC is specified in this Schedule, which has the effect of exempting AUSTRAC from the operation of the FOI Act in respect of:

> … documents concerning information communicated to it under section 16 of the *Financial Transaction Reports Act 1988* or section 41 or 49 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*[.]

26. Further, s 7(1)(c) provides that a reference in the Privacy Act to an 'act or practice' engaged in by a body includes an 'act or practice' engaged in by an agency specified in Division 1 of Part II of Schedule 2 to the FOI Act, other than an act done, or a practice engaged in, in relation to a record in relation to which the agency is exempt from the operation of that Act.

27. Relevantly for present purposes, this means that AUSTRAC is not subject to the Privacy Act in relation to its own acts and practices in respect of Suspicious Matter Reports (SMRs) provided to it under s 41 of the AML/CTF Act or further information provided about a SMR by a reporting entity in response to a notice issued by AUSTRAC to the entity under s 49 of the Act.

ASIO, ASIS, ASD and ONI

28. Section 7(1)(a)(i) provides that a reference in the Privacy Act to an 'act or practice' engaged in by a body does not include an 'act or practice' engaged in by an agency specified in Division 1 of Part I of Schedule 2 to the FOI Act. ASIO, ASIS, ASD and ONI are specified in this Schedule.

29. Further, s 7(1)(f) provides that a reference in the Privacy Act to an 'act or practice' does 'not include a reference to an act done, or a practice engaged in, in relation to a record that has originated with, or has been received from … an intelligence agency' [which includes ASIO, ASIS, ASD and ONI – see the definition of 'intelligence agency' in s 6(1)].

30. This means that ASIO, ASIS, ASD and ONI are not subject to the Privacy Act in relation to their own acts or practices nor are other APP entities subject to the Privacy Act in relation to their handling of an ASIO, ASIS, ASD or ONI record.

31. The Privacy Act also deals specifically with the disclosure of personal information by other APP entities to these agencies. Sections 7(1A) and 7(1B) of the Privacy Act provide as follows:

> (1A) Despite subsections (1) and (2), a reference in this Act (other than section 8) to an act or to a practice does not include a reference to the act or practice so far as it involves the disclosure of personal information to:
>
> (a) the Australian Security Intelligence Organisation; or
>
> (b) the Australian Secret Intelligence Service; or
>
> (c) the Australian Signals Directorate.
>
> (1B) Despite subsections (1) and (2), a reference in this Act (other than section 8) to an act or to a practice does not include a reference to the act or practice by an agency with an intelligence role or function (within the meaning of the *Office of National Intelligence*

Act 2018) so far as it involves the disclosure of personal information to the Office of National Intelligence.

32. The legal effect of ss 7(1A) and 7(1B) is apparent when read with key definitional provisions in the Privacy Act such as s 13(1)(a), which expressly refers to 'an act or practice' of an APP entity. Section 13 stipulates the circumstances in which, for the purposes of the Privacy Act, an 'act or practice' engaged in by a relevant body amounts to 'an interference with the privacy of an individual'. It follows from s 13, read with ss 7(1A) and 7(1B), that no complaint may be made to the Australian Information Commissioner about a disclosure of personal information by an APP entity to ASIO, ASIS, ASD or ONI.

AGO and DIO

33. Section 7(1)(ca) provides that a reference in the Privacy Act to an 'act or practice' engaged in by a body includes an 'act or practice' engaged in by a part of Defence specified in Division 2 of Part I of Schedule 2 to the FOI Act, other than an act done, or a practice engaged in, in relation to the activities of that part of the Department. AGO and DIO are specified in this Schedule.

34. Further, s 7(1)(g) provides that a reference in the Privacy Act to an 'act or practice' does 'not include a reference to an act done, or a practice engaged in, in relation to a record that has originated with, or has been received from AGO or DIO.

35. This means that AGO and DIO are not subject to the Privacy Act in relation to their acts or practices arising out of their intelligence activities nor are other APP entities subject to the Privacy Act in relation to their handling of an AGO or DIO record.

36. We note, however, that AGO and DIO do not share the protection afforded by s 7(1A) of the Privacy Act in relation to disclosures to certain intelligence agencies by other APP entities.

ACC

37. Section 7(1)(a)(iv) provides that a reference in the Privacy Act to an 'act or practice' engaged in by a body does not include an 'act or practice' engaged in by the ACC.

38. Further, s 7(1)(h) provides that a reference in the Privacy Act to an 'act or practice' does 'not include a reference to an act done, or a practice engaged in, in relation to a record that has originated with, or has been received from … the ACC or the Board of the ACC'.

39. This means that the ACC is not subject to the Privacy Act in relation to its acts or practices nor are other APP entities subject to the Privacy Act in relation to their handling of an ACC record.

PART 3: PRIVACY IMPACT ANALYSIS – PRIVACY IMPLICATIONS AND ANALYSIS OF PERSONAL INFORMATION FLOWS

40. In this section we identify and analyse the privacy implications arising from the introduction of the amendments proposed in the draft Bill (having regard to the Privacy Act limitations in respect of AUSTRAC, the ACC and intelligence agency

acts and practices as outlined above). We refer extensively to the APPs set out in Schedule 1 to the Privacy Act.

41. We omit discussion of several particular APPs in relation to the proposed amendments because the draft Bill will not make any change to the law in a way that would engage those APPs. On this basis, APP 1 (open and transparent management of personal information), APP 2 (anonymity and pseudonymity), APP 4 (unsolicited personal information), APP 7 (direct marketing), APP 9 (government related identifiers), APP 10 (quality of personal information) and APP 11 (security and retention) are not discussed in this PIA.

The aim of the changes to be made by the draft Bill

42. In general terms, we understand the intention of the draft Bill is to implement various recommendations made in the Statutory Review Report. The Report noted that the secrecy and access provisions in Part 11 of the AML/CTF Act are overly complex and impede information sharing and that this complexity generates considerable uncertainty, impeding the flow and use of financial intelligence for operational purposes and preventing the sharing of AUSTRAC information for other legitimate purposes.

43. The Report specifically considered the operation of the current 'tipping off' offence in s 123 of the AML/CTF Act. Currently a reporting entity under the Act must submit a SMR if, at any time while providing a designated service to a customer, the reporting entity forms a reasonable suspicion that the matter may be related to an offence against the Commonwealth, or a State or Territory (see s 41).

44. This SMR obligation brings with it a prohibition on 'tipping off'. This offence prohibits reporting entities from disclosing the fact that an SMR or SMR-related information is being, or has been, filed with AUSTRAC unless an exception applies, safeguarding against reporting entities 'tipping off' their customers that suspicious activity engaged in by the customer has been reported.

45. The Statutory Review Report made two recommendations in relation to Part 11:

> Recommendation 14.1 - develop a simplified model for sharing information collected under the AML/CTF Act that:
>
> - is responsive to the information needs of agencies tasked with combating ML/TF and other serious crimes
>
> - supports collaborative approaches to combating ML/TF and other serious crime at the national and international level, and
>
> - establishes appropriate safeguards and controls that are readily understood and consistently applied.
>
> Recommendation 14.2 - subject to appropriate controls and safeguards, the AML/CTF Act should be amended to permit reporting entities to disclose suspicious matter report related information to foreign parent entities and external auditors.

46. We are instructed that the intention of the draft Bill is to repeal and replace Part 11 of the AML/CTF Act to simplify information-sharing requirements, remove barriers to

collaboration between relevant agencies and enable wider and more efficient sharing of information to better detect, prevent and disrupt money-laundering, terrorism financing and other serious crimes.

47. In this sense it is important to note that, in the main, the draft Bill does not aim to expand the type or amount of information, including 'personal information' within the meaning of the Privacy Act, which is accessible by relevant agencies (and by certain organisations directly from AUSTRAC) or reportable by the relevant organisations, nor does it significantly expand the number and type of agencies and / organisations that can access this information in specified circumstances.

48. Instead, it reformulates and clarifies the rules applying to the use and disclosure of AUSTRAC information by these agencies and organisations and creates further exceptions to the tipping off offence to enable reporting entities which are members of corporate groups to disclose to disclose SMRs to external auditors[11] and other members of their corporate groups.

The kinds of information to which the changes implemented by the draft Bill will apply

Secrecy and access provisions

49. One of the aims of the draft Bill is to broaden and simplify the definition of 'AUSTRAC information' in the AML/CTF Act, which is currently defined in s 5 of the Act as follows:

> ***AUSTRAC information*** means:
>
> (a) eligible collected information; or
>
> (b) a compilation by the AUSTRAC CEO of eligible collected information; or
>
> (c) an analysis by the AUSTRAC CEO of eligible collected information.

In turn, 'eligible collected information' is defined in s 5 of the Act as follows:

> ***eligible collected information*** means:
>
> (a) information obtained by the AUSTRAC CEO under:
>
> (i) this Act; or
>
> (ii) any other law of the Commonwealth; or
>
> (iii) a law of a State or Territory; or
>
> (b) information obtained by the AUSTRAC CEO from a government body; or
>
> (c) information obtained by an authorised officer under Part 13, 14 or 15; and includes FTR information (within the meaning of the *Financial Transaction Reports Act 1988*).

[11] Who have been appointed or engaged by the reporting entity to audit or review the entity's AML/CTF program.

50. It has been identified by the Department that the current definitions of 'AUSTRAC information' and 'eligible collected information' do not anticipate all of the ways in which information is collected or obtained by the AUSTRAC CEO. For example, it has been identified that the definition does not capture information that the CEO can receive from:

- a person who is not a reporting entity about a transaction that appears suspicious (eg a voluntary SMR)
- a person who wishes to 'dob-in' a reporting entity for an alleged breach of regulatory obligations and possible criminal offences under the AML/CTF Act and the Rules made under that Act
- international, multi-jurisdictional bodies with a law enforcement function (such as Europol and Interpol).

51. Under the draft Bill the above definitions will be repealed and replaced by the following (see item 39):

> ***AUSTRAC information*** means the following:
>
> (a) information obtained by, or generated by, an AUSTRAC entrusted person under or for the purposes of this Act;
>
> (b) information obtained by an AUSTRAC entrusted person under any other law of the Commonwealth or a law of a State or Territory;
>
> (c) information obtained by an AUSTRAC entrusted person from a government body;
>
> (d) FTR information (within the meaning of the *Financial Transaction Reports Act 1988*).

This new definition is intended to have broad coverage, extending to all types of information obtained or generated in an official capacity by an 'AUSTRAC entrusted person' as well as 'FTR information'.[12]

52. The concept of an 'AUSTRAC entrusted person' is new (see item 38) and extends, for example, to the AUSTRAC CEO, a member of the staff of AUSTRAC and a person engaged as a consultant under the AML/CTF Act.

53. 'AUSTRAC information' will include personal information as well as other types of information. 'Personal information' is defined in s 6(1) of the Privacy Act to mean:

> …. information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

---

12 Which is defined in s 3 of the *Financial Transaction Reports Act 1988* [FTR Act] to mean 'information obtained by the AUSTRAC CEO under Part II [of that Act] and includes information included in a notice under subsection 22(1) or in a copy of a record given under subsection 24(5)'.

54. The personal information that will be collected, used and disclosed under the proposed amendments may potentially include sensitive information in some cases. 'Sensitive information' is defined in s 6(1) of the Privacy Act to mean:

> (a) information or an opinion about an individual's:
> (i) racial or ethnic origin; or
> (ii) political opinions; or
> (iii) membership of a political association; or
> (iv) religious beliefs or affiliations; or
> (v) philosophical beliefs; or
> (vi) membership of a professional or trade association; or
> (vii) membership of a trade union; or
> (viii) sexual orientation or practices; or
> (ix) criminal record;
> that is also personal information; or
> (b) health information about an individual; or
> (c) genetic information about an individual that is not otherwise health information; or
> (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
> (e) biometric templates.

55. For example, it seems possible that information about an individual's political opinions or membership of a political association may be disclosed to or obtained by AUSTRAC in particular circumstances (such as where access to an individual's financial history indicates that he or she is regularly paying political party membership fees). For this reason, we have reflected this possibility in broad terms in our comments below although note that in some instances (including where s 41 operates) AUSTRAC's acts and practices with respect to certain records are not subject to Privacy Act obligations in any event.

56. Broadly speaking, the secrecy and access inserts to the draft Bill considered in this PIA concern the following activities relating to the handling of information comprising personal information by and between Commonwealth, State, Territory and foreign government agencies:

- the disclosure of information obtained under s 49 of the AML/CTF Act by 'entrusted investigating officials' (see item 49 – proposed s 50A)[13]

[13] 'Entrusted investigating official' is defined to mean the Commissioner of the AFP, the Chief Executive Officer of the ACC, the Commissioner of Taxation, the Comptroller General of Customs, the Integrity Commissioner or an investigating officer (see item 42). 'Investigating officer' is defined in s 5 of the AML/CTF Act to mean a taxation officer, an AFP member, a customs officer (other than the Comptroller General of Customs), an examiner or member of the staff of the ACC or an Australian Commission for Law Enforcement Integrity officer.

- the use and disclosure of AUSTRAC information by AUSTRAC entrusted persons (see item 50 – proposed s 121)
- authorisation arrangements for 'specified officials of a Commonwealth, State or Territory agency' to access (ie collect) AUSTRAC information (see item 54 – proposed s 125)
- the use and disclosure of AUSTRAC information by officials of a Commonwealth, State or Territory agency after it has been obtained by them in accordance with proposed s 121(3), proposed s 125 or proposed s 126 (see items 50 and 54 – proposed s 126)
- the disclosure of AUSTRAC information to the government of a foreign country or to a foreign agency[14] by the AUSTRAC CEO or the agencies listed in proposed s 127(2) (see item 54 – proposed s 127).

57. The secrecy and access inserts to the draft Bill considered in this PIA also provide for some limited circumstances where AUSTRAC entrusted persons may disclose AUSTRAC information to other persons who are not AUSTRAC entrusted persons[15] for the purposes set out in proposed s 121(2), which include disclosure for the purposes of the AML/CTF Act and disclosure for the purposes of the performance of the functions of the AUSTRAC CEO (AUSTRAC purposes). Conditions may be imposed in relation to the recipient's subsequent handling of the disclosed information and the breach of any such conditions is an offence (see item 50 – proposed ss 121(4) and 121(6)).

Tipping off offence provisions

58. The new exceptions to the tipping off offence proposed to be inserted by the draft Bill will permit a new type of disclosure to be made, relating to the giving of SMRs to AUSTRAC. As an SMR will include personal information – both for customers as individuals and potentially also where the information to be disclosed is about individuals who are associated with other customers – the tipping off offence provisions in the draft Bill considered in this PIA concern the following activity relating to the handling of information comprising personal information:

- the disclosure of SMRs by reporting entities that are 'organisations' within the meaning of the Privacy Act to external auditors and other members of their designated business group or corporate group (see item 18 – proposed

---

14 'Foreign agency' is defined to mean 'a government body that has responsibility for intelligence gathering for a foreign country or the security of a foreign country, a government body that has responsibility for law enforcement in a foreign country or a part of a foreign country, a government body that has responsibility for the protection of the public revenue of a foreign country, a government body that has regulatory functions in a foreign country, the European Police Office (Europol), the International Criminal Police Organization (Interpol) or an international body prescribed by the regulations for the purposes of this paragraph' (see item 42).

15 We are instructed that this is intended to facilitate a more collaborative approach between AUSTRAC and the private sector and academia, such as through the ongoing work of AUSTRAC's public/private partnership, the Fintel Alliance. Some of the recipients of this information will be 'organisations' within the meaning of the Privacy Act.

amendments to ss 123(1) and (2), item 23 – proposed new ss 127(5B) and 127(5C) and item 25 – proposed amendments to ss 123(7) and 123(7AA) and proposed new ss 123(7AB) and 123(7AC).

59. Our comments below address the Privacy Act implications of each of these kinds of activities, having regard to relevant APP obligations.

Collection of personal information

60. APP 3 imposes limits on the collection of personal information by APP entities. Of particular relevance in the present circumstances, APP 3.1 requires that an APP entity that is an agency must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of its functions or activities.

61. With respect to sensitive information, the effect of APP 3.3 and 3.4(a) in the particular circumstances arising here is that an agency within the meaning of the Privacy Act will be permitted to collect sensitive information, without consent, to the extent that this collection is required or authorised by the draft Bill or otherwise by the legislation it amends.

62. Alternatively, under APP 3.4(d), the collection of sensitive information may proceed without consent where:

> (d) the APP entity is an enforcement body and the entity reasonably believes that:
>
> (i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or
>
> (ii) otherwise — the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities …

63. As noted above, the proposed amendments relate specifically to the following collection of personal information:

- the collection of AUSTRAC information by 'specified officials of a specified Commonwealth, State or Territory agency'.

64. Proposed s 125 of the draft Bill will relevantly permit the AUSTRAC CEO to give written authorisation for specified officials of a Commonwealth, State or Territory agency to access AUSTRAC information for the purposes of performing the agency's functions and duties and exercising the agency's powers. In the case of State and Territory agencies, such an authorisation may only be given where the head of the relevant agency has given a written undertaking that agency officials will comply with the APPs in respect of AUSTRAC information obtained under the authorisation or proposed s 126(2) (which relevantly permits a person holding AUSTRAC information to disclose it to another official in the same agency for the same purposes). Related to this, item 40 will insert a definition of 'Commonwealth, State or Territory agency' into s 5 of the AML/CTF Act.

65. As noted above, this PIA focuses on the effect that the provisions in the draft Bill may have on the APP obligations of Commonwealth agencies (as it is only these agencies that are subject to the Privacy Act directly). In terms of APP compliance, proposed s 125 will have the following effects in relation to APP 3:

- to the extent it will authorise the collection of personal (other than sensitive) information by authorised agency officials, such collection will be consistent with APP 3.1 provided that the collection is reasonably necessary for, or directly related to, one or more of the functions or activities of the collecting agency
- to the extent it will authorise the collection of sensitive information by authorised agency officials, such collection will be consistent with APP 3.4(a), because the draft Bill will operate to authorise the collection of this information for the purposes described in proposed s 125(1)
- to the extent it will authorise the collection of sensitive information by authorised agency officials working in 'enforcement bodies' (relevantly defined in s 6(1) of the Privacy Act to include agencies such as the AFP, the ACC and the Department), it is possible that APP 3.4(d) would also be triggered – however, this would need to be determined on a case by case basis, having regard to:
  - the particular agency (noting, for example, that not all of the Department's activities generally are 'enforcement related activities' as defined in s 6(1) of the Privacy Act)
  - the purposes for which the authorisation is proposed to be given (noting, for example, that APP 3.4(d)(i) imposes 'reasonably necessary for, or directly related to' requirements in relation to any collection by the Department, which are stricter requirements than for collection by other agencies).

66. Importantly, APP 3.5 requires that the collection of information be done by means which are both lawful and fair.

Recommendation 1 – Development of authorisation form and associated material
The Department and / or AUSTRAC develop a template form and associated guidance material to ensure that authorisations will be given to agency officials only where the requirements of proposed s 125 are met.

Providing notice of collection

67. APP 5 requires APP entities, at or before the time of collection or as soon as practicable after they collect personal information about an individual, to take such steps as are reasonable in the circumstances to notify the individual of the matters specified in subclause 5.2, or to otherwise ensure the individual is aware of any such matters. This obligation applies to any collection of personal information, regardless of whether the information is collected directly from the individual. It will

therefore apply with respect to all forms of collection of such information under the draft Bill as discussed above.

68. We assume that where AUSTRAC information is to be used or disclosed for law enforcement or intelligence purposes, and therefore needs to be collected for these same purposes, this would ordinarily need to occur without the knowledge of the individual who is the subject of the information. The covert nature of these activities would, by definition, ordinarily mean that it is not reasonable to alert the individual concerned (or other individuals, such as their associates) to the collection of personal information about them. Presumably, to do so would risk defeating the law enforcement or intelligence purpose and put the individuals on notice of any intelligence that law enforcement authorities may have collected concerning their activities using these methods.

69. For the above reasons, we consider that APP 5 would apply in the present circumstances in the same way that it is presumably currently applied by agencies in criminal investigation, intelligence and other law enforcement contexts. We do not consider that any additional steps are required to ensure APP 5 compliance.

Use and disclosure of personal information

70. APP 6.1 provides that if an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless the individual consents or APP 6.2 or 6.3 apply. Relevantly, APP 6.2(b) provides for use or disclosure of information 'required or authorised by or under an Australian law or a court/tribunal order', and APP 6.2(e) provides for use or disclosure where 'the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body'.

71. As noted above, the proposed amendments relate specifically to the following uses and disclosures of personal information:

- the disclosure of information obtained under s 49 of the AML/CTF Act by 'entrusted investigating officials'
- the use and disclosure of AUSTRAC information by AUSTRAC entrusted persons
- the use and disclosure of AUSTRAC information by officials of a Commonwealth, State or Territory agency
- the disclosure of AUSTRAC information to the government of a foreign country, or to a foreign agency by the AUSTRAC CEO or those agencies listed in proposed s 127(2)
- the disclosure of SMRs comprising personal information by reporting entities.

72. For the reasons set out in paragraphs 25-39 above, not all of the above agency activities are governed by the APPs. In particular, this is the case to the extent that:

- the CEO of the ACC or an examiner or member of the staff of the ACC is an 'entrusted investigating official' disclosing information obtained under s 49 of the AML/CTF Act
- AUSTRAC entrusted persons are using or disclosing AUSTRAC information containing information contained in documents communicated to AUSTRAC under s 16 of the FTR Act or ss 41 or 49 of the AML/CTF Act
- officials in ASIO, ASIS, ASD, ONI or the ACC, or AGO or DIO (in respect of carrying out their particular activities within Defence), are using or disclosing AUSTRAC information obtained by them from AUSTRAC entrusted persons
- the AUSTRAC CEO is disclosing AUSTRAC information containing information contained in documents communicated to AUSTRAC under s 16 of the FTR Act or ss 41 or 49 of the AML/CTF Act to a foreign agency
- ASIO, ASIS, ASD, ONI or the ACC, or AGO or DIO (in respect of carrying out their particular activities within Defence), are disclosing AUSTRAC information to a foreign agency.

73. However, the question of APP 6 compliance arises in respect of:

- other 'entrusted investigating officials' disclosing information obtained under s 49 of the AML/CTF Act
- AUSTRAC entrusted persons using and disclosing other types of AUSTRAC information comprising personal information
- other Commonwealth agencies using and disclosing AUSTRAC information comprising personal information
- other Commonwealth agencies disclosing AUSTRAC information to a foreign agency
- organisations that are reporting entities disclosing SMRs comprising personal information
- organisations using and disclosing AUSTRAC information comprising personal information that was obtained by them for AUSTRAC purposes (see further paragraph 57 above).

74. There will be instances where personal information obtained through the mechanisms outlined in the draft Bill will be used or disclosed for the purpose for which that information is collected, meaning that APP 6.1 applies. This could be the case where, for example:

- 'specified officials of a specified Commonwealth, State or Territory agency' are given written authorisation to access AUSTRAC information for the purposes of performing the agency's functions and duties and exercising the agency's powers under proposed s 125 of the draft Bill
- 'entrusted investigating officials' are disclosing information obtained under s 49 of the AML/CTF Act for the purposes of, or in connection with, the performance

or exercise of the person's functions, duties or powers as an entrusted investigating official under proposed s 50A(2) of the draft Bill

- a person to whom AUSTRAC information has been given for AUSTRAC purposes under proposed s 121 of the draft Bill uses or discloses the information for those purposes (and subject to any conditions imposed under proposed s 121(4)).

75. However, in circumstances where information subject to the secrecy obligations in the draft Bill has been collected by a relevant person for one (lawful) purpose and is proposed to be used or disclosed for a different purpose, the exception in APP 6.2(b) will apply where the obtained information is used or disclosed for the secondary purposes contemplated under the draft Bill or under existing provisions of the legislation it amends.

76. In particular circumstances, the requirements for the operation of APP 6.2(e) may additionally be satisfied. It is not possible to assess specific factual scenarios under this PIA (which assesses the general operation of draft Bill provisions as currently proposed).

77. The Bill applies secrecy protections to the handling of information obtained under s 49 of the AML/CTF Act, AUSTRAC information and SMRs.

78. In preparing this PIA we have specifically considered the questions of whether the secrecy and access regimes proposed to be added or amended under the draft Bill (ie proposed ss 50A, 121, 125, 126 and 127) and the revised tipping off offence (ie items 18, 23 and 25) would engage the 'authorised or required by law' exception in APP 6.2(b).

79. The *APP guidelines* state (at [B.130]-[B.132]) that:

> An APP entity that is 'authorised' under an Australian law or a court/tribunal order has discretion as to whether it will handle information in a particular way. The entity is permitted to take the action but is not required to do so. The authorisation may be indicated by a word such as 'may', but may also be implied rather than expressed in the law or order... An act or practice is not 'authorised' solely because there is no law or court/tribunal order prohibiting it. Nor can an act or practice rely solely on a general or incidental authority conferred by statute upon an agency to do anything necessary or convenient for, or incidental to or consequential upon, the specific functions and powers of the agency. The reason is that the purpose of the APPs is to protect the privacy of individuals by imposing obligations on APP entities in handling personal information. A law will not authorise an exception to those requirements unless it does so by clear and direct language.

80. Having regard to the above, we think it is clear that any use or disclosure of information done consistently with the terms of these proposed sections is 'authorised by law' for the purposes of APP 6.2(b). Each of those sections contains exceptions to prohibitions on use and / or disclosure which specifically operate to permit named persons (ie agency officials or reporting entities) to use or disclose information in certain prescribed circumstances.

Recommendation 2 – Development of processes to ensure compliance with new arrangements

That consideration be given by the Department and AUSTRAC to developing processes to ensure that all 'entrusted investigating officials', 'AUSTRAC entrusted persons' and designated entities are aware of their obligations under the proposed amendments including under the revised secrecy and access arrangements.

Cross-border disclosure of personal information

81. Proposed s 127 and ss 123(7) and 123(7AA) relate specifically to the disclosure of certain information to entities located overseas. In the case of proposed s 127, these are foreign agencies. In the case of proposed ss 123(7) and 123(7AA) these are overseas bodies corporate within the same corporate group as the reporting entity.

82. APP 8.1 provides that, subject to exceptions set out in APP 8.2, an APP entity must take such steps as are reasonable in the circumstances to ensure that an overseas entity does not breach the APPs (excluding APP 1) before it discloses personal information to that overseas entity.

83. Relevantly, APP 8.2(c) provides that APP 8.1 does not apply where the disclosure is 'required or authorised by or under an Australian law or a court/tribunal order'.

84. The *APP guidelines* explain the definition of 'overseas entity' for the purpose of APP 8 (at [8.5]):

> 8.5 Under APP 8.1, an 'overseas recipient' is a person who receives personal information from an APP entity and is:
>
> - not in Australia or an external Territory
> - not the APP entity disclosing the personal information, and
> - not the individual to whom the personal information relates.

85. The limitations we identify in paragraph 72 (dot points 4 and 5) are again relevant here. However, to the extent that other Commonwealth agencies are disclosing AUSTRAC information to a foreign agency consistently with proposed s 127 or organisations are disclosing SMRs comprising personal information to overseas recipients consistently with proposed ss 123(7) and 123(7AA), we think it is clear that any such disclosure of information is 'authorised by law' for the purposes of APP 8.2(c).

Recommendation 3 – Development of guidance to reporting entities about overseas disclosure

That consideration be given by the Department and AUSTRAC to providing reporting entities with specific guidance on ensuring compliance with APP 8 obligations when disclosing any personal information to any separate legal entities located overseas.

Access and correction

86. APP 12 imposes requirements on APP entities to permit individuals to access personal information about them which the entity holds in certain circumstances. Similarly, APP 13 imposes requirements on APP entities in defined circumstances to correct personal information they hold.

87. The draft Bill does not contain any new provisions directly relating to access and correction of information held by Commonwealth agencies and, as above, we assume that existing practices by relevant agencies and organisations are conducted in accordance with APP 12 and 13.

88. Given the nature of the activities dealt with in the draft Bill, it is likely that much of the personal information that may be held by relevant Commonwealth agencies as a result of the operation of these provisions will be exempt from disclosure under the FOI Act and therefore fall within the exception in APP 12.2(a).

89. Similarly, given the context in which the personal information is obtained, it is difficult to conceive of any reasonable steps that may be required to correct such personal information under APP 13.1.

OVERALL EFFECT AND IMPACT OF THESE CHANGES AND RELATED RECOMMENDATIONS

90. It can be seen from the above discussion that the proposed changes to Commonwealth law set out in the draft Bill raise various potential privacy issues for consideration, both for those Commonwealth agencies subject to APP requirements and for those organisations that are reporting entities or receive AUSTRAC information for AUSTRAC purposes.

91. In many instances, to the extent that these APP entities (ie Commonwealth agencies and organisations) need to engage in any new acts and practices associated with the handling of personal information in order to implement the changed arrangements set out in the draft Bill, these activities will be APP-compliant. In their proper application, the draft Bill provisions will ensure that any new collections of personal information for these purposes are relevantly associated with the functions and activities of these agencies and relevant organisations having recourse to the mechanisms in the draft Bill. They will also ensure that personal information is used and disclosed by agencies and by organisations (both reporting entities and those receiving AUSTRAC information for AUSTRAC purposes) either

for the purpose for which it was originally collected or as required or authorised by or under law.

92. There are various measures contained in the draft Bill to ensure that the collection, use and disclosure is consistent with the requirements of the Privacy Act, such as by engaging the 'authorised by law' exception in APP 3.4(a) and APP 6.2(b).

93. The draft Bill also contains various measures which would seem to be directed at ensuring that the collection, use and disclosure of the information is not permitted beyond what is necessary to facilitate and achieve the identified policy objectives, for example:

- collection of personal information is only authorised for limited purposes which we understand are intended to align with these policy objectives
- there are limitations on the parties to whom AUSTRAC information can be disclosed under the proposed provisions including specific authorisation requirements which will be privacy protective provisions
- express secrecy offences will apply to the mishandling of personal information beyond the permissions set out in the draft Bill.

94. While the proposed draft Bill will clearly have privacy impacts (and, in practice, would serve no purpose if it did not) we think that these impacts are balanced against the policy objectives they serve and there are mechanisms included in the draft Bill that appropriately define and limit its overall privacy impacts.

95. We also recommend that the Department give further consideration to various matters, as set out below:

Recommendation 1 – Development of authorisation form and associated material
The Department and / or AUSTRAC develop a template form and associated guidance material to ensure that authorisations will be given to agency officials only where the requirements of proposed s 125 are met.
Recommendation 2 – Development of processes to ensure compliance with new arrangements
That consideration be given by the Department and AUSTRAC to developing processes to ensure that all 'entrusted investigating officials', 'AUSTRAC entrusted persons' and designated entities are aware of their obligations under the proposed amendments including under the revised secrecy and access arrangements.

Recommendation 3 – Development of guidance to reporting entities about overseas disclosure
That consideration be given by the Department and AUSTRAC to providing reporting entities with specific guidance on ensuring compliance with APP 8 obligations when disclosing any personal information to any separate legal entities located overseas.

HOME AFFAIRS PORTFOLIO

DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Legal and Constitutional Affairs Legislation Committee

14 February 2020

QoN Number: AMLCTF/005

Subject: The Office of the Australian Information Commissioner submission

Asked by: Senator Amanda Stoker

Question:

In its submission to the inquiry, the Office of the Australian Information Commissioner has recommended 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'. Can the department respond to this recommendation?

Answer:

New section 125 of the Bill empowers the Australian Transaction Reports and Analysis Centre (AUSTRAC) CEO to authorise officials from a 'Commonwealth, State or Territory agency' to access AUSTRAC information for the purposes of performing the agency's functions and duties and exercising its powers.

However, in accordance with proposed subsection 125(2), Commonwealth, State or Territory agencies may only access AUSTRAC information if the agency head provides a written undertaking to the AUSTRAC CEO that their officials will comply with the Australian Privacy Principles (APPs) in the *Privacy Act 1988* in dealing with AUSTRAC information. In effect, this obliges all individuals and entities that are permitted to access, use and disclose AUSTRAC information to do so in accordance with the APPs.

Furthermore, there are additional privacy safeguards that can be built into the AUSTRAC CEO's instrument of authorisation made under new section 125. For instance, the instrument of authorisation can limit the type of AUSTRAC information that can be accessed by the agency and its officials. This will ensure that specified officials only have access to AUSTRAC information that is necessary for them to perform their functions and duties.

HOME AFFAIRS PORTFOLIO

DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Legal and Constitutional Affairs Legislation Committee

14 February 2020

QoN Number: AMLCTF/006

Subject: The disclosure of AUSTRAC information overseas

Asked by: Senator Amanda Stoker

Question:

With respect to the disclosure of AUSTRAC information overseas, what safeguards are in place to protect the personal information of Australians? How will the proposed amendments to existing section 132 allow for effective disclosure of certain information while still providing confidence that the information is secure?

Answer:

New section 127 of the Bill deals with the disclosure of AUSTRAC information to foreign countries or foreign agencies by the AUSTRAC CEO or a prescribed Commonwealth, State or Territory agency. The disclosure of personal information to a foreign counterpart would still be subject to the Australian Privacy Principles (APPs) in the *Privacy Act 1988*. APP 8 outlines the steps an APP entity must take to protect personal information before it is disclosed overseas. For example, before disclosing personal information about an individual to a foreign counterpart, the APP entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where AUSTRAC information is disclosed to a foreign counterpart, the APP entity will be accountable for an act or practice of the foreign counterpart that would breach the APPs.

New subsection 127(1) of the Bill proposes to modify the effect of section 132, by making it discretionary, rather than mandatory, for the AUSTRAC CEO to seek an undertaking from an overseas government agency prior to disclosing AUSTRAC information. Despite the relaxing of this requirement, as mentioned above, disclosure of the AUSTRAC information to foreign counterparts will be subject to the protections of APP 8.

In addition to this, AUSTRAC is in the process of developing robust policies around the CEO's discretion to disclose information overseas. These will be based on the requirement in new paragraph 127(1)(b) that any disclosure by the CEO must still be considered appropriate, in all the circumstances, to do so.

HOME AFFAIRS PORTFOLIO

DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY WRITTEN QUESTION ON NOTICE

Legal and Constitutional Affairs Legislation Committee

14 February 2020

QoN Number: AMLCTF/007

Subject: Support for industry

Asked by: Senator Amanda Stoker

Question:

How will industry organisations and other stakeholders be supported to implement the measures proposed in the bill?

Answer:

During the development of these legislative reforms, the Department of Home Affairs and the Australian Transaction Reports and Analysis Centre (AUSTRAC) consulted extensively and worked closely with relevant industry associations.

The Bill provides for staggered commencement (6 months for Schedule 1, Parts 1 to 4 and 18 months for Schedule 1, Part 5) providing sufficient time and opportunity for industry to implement the measures proposed in the Bill. During this time, AUSTRAC will conduct outreach in the form of guidance and industry engagement to support industry and other stakeholders to implement the measures proposed in the Bill. AUSTRAC will also consult with reporting entities on exposure draft AML/CTF Rules required to implement provisions in the Bill.