Australian Government

Office of the Privacy Commissioner

Submission by the Office of the Privacy Commissioner

to the Senate Legal and Constitutional Committee

Inquiry into the Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005

March 2006

Summary

a) The Office accepts the public interest in ensuring that Australia's financial regulatory systems and procedures incorporate appropriate responses to the risks of money laundering and terrorist financing (paragraphs 27-30).

b) When developing such responses, it is essential that any measures which may adversely affect the privacy of Australians are necessary and proportionate to both the nature and degree of risk that exists (27-30).

c) The Exposure Bill would benefit significantly from having a Privacy Impact Assessment conducted (31-32).

d) This submission notes that some, but probably not all, reporting entities will have obligations under the Privacy Act 1988 as to how they handle personal information collected pursuant to Exposure Bill. It remains unclear though, whether the coverage and content of the NPPs is adequate for the purposes of the regime envisaged under the Exposure Bill (16-26).

e) This submission proposes a range of options for introducing consistent privacy regulation over all entities that may handle personal information under the terms of the Exposure Bill (33-39).

f) The Office suggests that any prescribed period for which reporting entities must retain personal information be determined with reference to the specific purpose for which that information was initially collected (40-41).

g) The Office submits that the replacement of the existing regulation with new legislation, with its greater scope and impact, does not, of itself, necessarily justify the continuance of the present data-sharing arrangements so as to permit access to the welfare and assistance agencies (42-46).

h) It is recommended that access by other agencies to AUSTRAC-held data be limited to more precisely defined purposes and be subject to additional transparency and oversight (47-49).

i) The Office notes that the threshold amount for a significant transaction report has remained constant for over 15 years and may warrant re-examination. The Office also suggests that examination be made of the provision in the Exposure Bill concerning the making of regulations prescribing 'threshold transactions' of less than $10,000 value (50-54).

Inquiry into the Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner (the Office) is an independent statutory body responsible for promoting an Australian culture that respects privacy. The Office, established under the *Privacy Act 1988 (Cth)* (Privacy Act), has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses. The Office also has responsibilities under the Privacy Act in relation to credit worthiness information held by credit reporting agencies and credit providers, and personal tax file numbers used by individuals and organisations.

Introduction

2. The Office welcomes the opportunity to make this submission to the Senate Legal and Constitutional Committee's inquiry into the Exposure draft of the *Anti-Money Laundering and Counter-Terrorism Financing Bill 2005* (the Exposure Bill).
3. At the time of writing this submission, the Office has not had opportunity to consider the draft rules and guidelines attached to the Exposure Bill package. The Office intends to provide a submission to the review being conducted by the Attorney-General's Department and will take that opportunity to comment on the draft rules and guidelines, as well as other matters of detail.

Scope of existing regulation

4. At present, the *Financial Transactions Reports Act 1988* (FTR Act) regulates the reporting of certain financial transactions to AUSTRAC. The FTR scheme was designed to protect the Australian financial system against tax evaders and money launderers.[1] At present, a number of agencies, including welfare and assistance agencies, utilise the financial transactions data currently collected by AUSTRAC under the FTR Act. As an Australian Government agency, AUSTRAC is covered by the Privacy Act.
5. The Office understands that, in the 2004-05 financial year, AUSTRAC received 17,212 suspect transaction reports, 2,288,373 significant cash transaction reports and 10,243,774 international funds transfer

[1] See http://www.austrac.gov.au/ftr_act/index.html

instructions.[2] The Offices notes that the various categories of reporting have increased significantly since the regime was established.

Scope and effect of the Exposure Bill

6. The Office understands that the Exposure Bill aims to enact the Australian Government's response to the recommendations of the Financial Action Task Force (FATF) on Money Laundering.[3] The Exposure Bill requires, *inter alia* 'reporting entities' that provide 'designated services' to:
    - carry out identification and verification procedures concerning individuals before providing that service;
    - report to AUSTRAC on 'suspicious matters', transactions that meet threshold criteria[4] and international funds transfer instructions;
    - develop and implement anti-money laundering and counter-terrorism financing programs for the purpose of identifying and "materially mitigating" risks; and
    - maintain ongoing "due diligence" of the risk profile of their clients and report suspicious behaviour detected by such surveillance to AUSTRAC.
7. The Exposure Bill, as the Office understands it, provides a legislative framework, with implementation to proceed in two tranches. Operational details will be prescribed by binding AML/CTF Rules, made under section 191 of the Exposure Bill. The Exposure Bill (and related Rules) will, if enacted, supersede the FTR Act and significantly extend the reach and the impact of the FTR Act by extending the obligations on existing reporting entities and introducing new entities to its regulation.
8. AUSTRAC will remain the Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) regulator, with broad powers that include, for example, the authority to determine which federal, state or territory agencies will have access to the personal information it collects.[5]

Impact of Exposure Bill on the handling of personal information

9. If enacted in its current form and with both tranches implemented, the Exposure Bill will impose personal information collection and disclosure obligations on far more entities than is currently the case under the FTR Act. If an organisation, regardless of type, provides a prescribed form of 'designated service' then it would be subject to the provisions introduced by the Exposure Bill. Section 6 provides two tables containing 64 'designated services' which, if performed, will bring the entity within the ambit of the proposed legislation.

[2] AUSTRAC Annual Report 2004-05, pp 17-18
[3] See http://www.fatf-gafi.org/pages/0,2987,en_32250379_32235720_1_1_1_1_1,00.html
[4] Namely, transactions involving amounts greater than $10,000 in either cash or e-currency (or less than $10,000 if provided for by regulation) and involving the provision of a designated service.
[5] Division 4 of Part 11 of the Exposure Bill.

10. Obligations that may affect the handling of personal information by 'reporting entities' include:

    - the collection of personal information under the identification procedures in Part 2 (*Identification procedures etc*);
    - disclosing to AUSTRAC reports of certain matters in Parts 3 (*Reporting obligations of reporting entities*) and 4 (*Reports about cross-border movements of physical current and bearer negotiable instruments*);
    - ongoing monitoring of the provision of designated services (including to individuals) as part of ongoing customer due diligence obligations under Part 7 (*Anti-money laundering and counter-terrorism financing programs*); and
    - retention obligations of Parts 2 and 10 (*Record keeping requirements*).

11. For example, in section 39(1)(d) of the Exposure Bill, a reporting entity must disclose to AUSTRAC reports of personal information concerning transactions if it forms a suspicion, on 'reasonable grounds', that the information may be relevant to:

    (i) an investigation concerning taxation laws;

    (ii) an offence against a law of the Commonwealth or of a Territory; or

    (iii) may be of assistance to the enforcement of the *Proceeds of Crime Act 2002*.

12. The Office notes that some of these prescribed reasonable grounds for disclosure are for purposes other than AML/CTF. It is useful to take into account the different policy drivers that may underpin such provisions, for example, the protection of public revenue, when considering the Exposure Bill, as the effects of such provisions are likely to be distinct from addressing AML/CTF risks.

13. The overall effect of these various provisions would be to make it mandatory for reporting entities to collect personal information about individuals, retain that personal information for extended periods, and to disclose that information to AUSTRAC, which may, in turn, make it available to a range of government agencies. Given the very large number of reports to AUSTRAC, it seems likely that most affected individuals and the transactions they undertake will not be related to money laundering or terrorist financing activities.

14. For individuals, this reduces their degree of control over their personal information, as they have no choice (and in many instances, perhaps no awareness) as to how their personal information is handled, other than to choose not to participate in a given transaction.

15. Further, as a wider range of reporting entities will be collecting a greater volume of personal information and providing that to AUSTRAC, this may result in the establishment of a centralised database of a significant percentage of the financial transactions entered into by Australians. From

this data, it could be possible to create a rich data trail of individuals' interactions in the economy.

Application of the Privacy Act to AML/CTF regulation

16. While AUSTRAC and other Australian Government agencies are covered by the IPPs, the ten National Privacy Principles (NPPs) in the Privacy Act regulate the information-handling practices of private sector 'organisations'. These organisations include businesses with a turnover greater than $3 million, as well as all businesses that provide a health service or which trade in personal information. Generally, a business with a turnover of $3 million or less (that is, a small business) would not fall within the jurisdiction of the NPPs unless it provided a health service or traded in personal information.[6]

17. The Office notes that those reporting entities which fall within the definition of "organisation" for the purposes of the Privacy Act will have obligations under the NPPs as to how they handle personal information. It remains unclear though, whether the coverage and content of the NPPs is adequate for the purposes of the regime envisaged under the Exposure Bill. In some cases, relevant reporting entities may not be covered. It may be appropriate to consider whether all reporting entities should have privacy regulations imposed given the mandatory nature of the collection and the sensitivity of the personal information.

Use and disclosure of personal information

18. NPP 2 gives effect to the underlying privacy principle that personal information should, in general, only be used or disclosed for the purpose for which it was initially collected. That NPP recognises that, in certain circumstances, it may be in the public interest for personal information to be used or disclosed for other purposes, and provides a range of exceptions to the general principle. These exceptions include where the use or disclosure is:

    - for a related secondary purpose within the individual's reasonable expectations (NPP 2.1(a));
    - with the individual's consent (NPP 2.1(b));
    - for the purpose of direct marketing (subject to conditions being met) (NPP 2.1(c));
    - required or authorised by law (NPP 2.1(g)); or
    - for purposes related to law enforcement (NPPs 2.1(f) and 2.1(h)).

19. Accordingly, organisations that would be required to collect personal information pursuant to the Exposure Bill, would then be regulated as to what other purposes they may use that information. However, as

[6] 'Small business' and 'small business operator' are defined in section 6D of the Privacy Act. More information on the coverage of the NPPs is available from http://www.privacy.gov.au/publications/IS12_01.html.

discussed above, the Privacy Act would not regulate the handling of this personal information by reporting entities that fall outside of its jurisdiction.

Notice and openness

20. NPPs 1.3 and 1.5 impose obligations on private sector organisation, when collecting personal information, to take reasonable steps to ensure that the individual is aware of a number of matters. These matters include the types of bodies to which the organisation usually discloses information of that kind, as well as any law that requires them to do so.
21. NPPs 5.1 and 5.2 require organisations to be open with individuals about the handling of their personal information, including by making available a document providing policies on such handling (including to whom it may disclose).
22. Compliance with these provisions will go some way to ensuring that individuals have an appropriate degree of understanding of how their personal information may be handled. However, those reporting entities that are not 'organisations' and hence not covered by the Privacy Act, will be under no obligation to comply with these principles.

Data quality and security, access and correction, and transborder flows

23. Similarly, the obligations imposed by the Privacy Act concerning data quality (NPP 3), data security (NPP 4), access and correction (NPP 6) and transborder data flows (NPP 9) will afford privacy protections only to the extent that they are applicable to the organisations. Many newly prescribed reporting entities will not be subject to this regulation.

Anonymity

24. NPP 8 establishes that individuals should have a choice as to whether they can remain anonymous when entering into transactions with an organisation, "wherever it is lawful and practicable". In contrast, the underlying policy thrust of the Exposure Bill is that individuals must identify themselves when participating in specific transactions. The range of transactions is expanded by the Exposure Bill.
25. The impact on the Australian community may be that personal information concerning many increasingly routine transactions, which are currently conducted anonymously, will be subject to mandatory collection by organisations and fall under the scrutiny of one or more government agencies. The extent to which individuals will be able to conduct their affairs on the basis of comparative anonymity may be significantly reduced.
26. Whether such an outcome is warranted can only be determined by careful consideration of competing public interests.

Ensuring an appropriate response to AML/CTF risks

27. The Office accepts the public interest in ensuring that Australia's financial regulatory systems and procedures incorporate appropriate responses to the risks of money laundering and terrorist financing. When developing such responses, it is essential that any measures which may adversely affect the privacy of Australians are necessary and proportionate to both the nature and degree of risk that exists.

28. The Office also notes that the effective implementation of legislative measures for AML/CTF purposes will depend in large part on the willing cooperation of the business community in providing critical financial data to law enforcement agencies.

29. This, in turn, will be underpinned by the understanding and confidence on the part of the community as to what happens to their financial data. It should be recognised that survey research conducted for the Office has found that the community is most reluctant to provide personal financial information to others.[7] A lack of confidence in how personal information is handled may have unintended and undesirable effects on the economy. For example, the Office's community attitude research has shown that a significant portion of the community are likely to not deal with organisations if they feel their personal information will not be handled appropriately.[8]

30. In recognition of the importance of ensuring that any measures taken are necessary and proportionate, the Exposure Bill would benefit from a rigorous analysis directed at assessing whether its provisions constitutes an appropriate way of meeting the underlying policy objectives. In very general terms, this analysis could usefully be directed at meeting the following questions:

    - Is the scope of the personal information handling proposed in the Exposure Bill reasonably connected to countering money laundering and terrorist financing?
    - Are the means limiting the right to privacy no more than is necessary to achieve the objective?
    - Can measures be adopted that reduce the risks posed to privacy or afford specific additional privacy protections to the acts and practices in question?

Privacy Impact Assessment

31. One potentially useful mechanism for examining the appropriateness of the Exposure Bill would be to conduct a formal Privacy Impact Assessment (PIA). A PIA is an assessment tool that describes, in detail, the personal information flows in a project, and analyses the possible

[7] See, community attitude research conducted for the Office in 2001 and 2004 (respectively at http://www.privacy.gov.au/publications/rcommunity.html and http://www.privacy.gov.au/publications/rcommunity/index.html).

[8] See, http://www.privacy.gov.au/publications/rcommunity/chap6.html.

privacy impacts of the project. A PIA may assist in identifying and evaluating the impact of such matters as the Exposure Bill's coverage and issues around uses and disclosures of personal data.

32. Ideally, a PIA should be conducted by an independent expert specialising in privacy issues and the conduct of PIAs.

Privacy regulation for the AML/CTF scheme

33. Effective privacy protections should play an essential role in the AML/CTF scheme, particularly to assist in retaining community confidence in the financial sector in respect of its ability to appropriately protect the personal information of its customers.

34. The Office notes that, given the cross-jurisdictional nature of Australian privacy regulation, a number of agencies, organisations and individuals, acting in accordance with the provisions of the Exposure Bill in its present form, will have differing privacy obligations, depending on, for example, whether they are in the public or private sectors.

35. The Office recognises the requirement imposed by section 99(2) of the Exposure Bill, permitting AUSTRAC to require state and territory bodies to which it discloses information to comply with the Information Privacy Principles. It is not clear to the Office how compliance with the IPPs could be legally enforceable and what mechanisms may offer remedies to individuals if their privacy is interfered with.

36. Further, the Office submits that to address the problem of inconsistent privacy regulation over current and envisaged reporting entities, the Exposure Bill should provide for the introduction of privacy provisions for all reporting entities, regardless of type or size. Such provisions should be consistent with those provided by the Privacy Act.

37. In recognition of the pervasiveness of the scheme, these protections could, in some places, afford a higher standard of protection than those offered by the Privacy Act, including by limiting the number of exceptions to a use or disclosure provision. Such an approach is in place for credit reporting information, Medicare and PBS claims information, and Tax File Numbers.[9]

38. There would appear a number of options for establishing an appropriate privacy framework in regard to the AML/CTF scheme. While the Office has not considered in depth the relative merits of each, these options could include:

    (a) Privacy protections could be adopted in a schedule to the Exposure Bill. To ensure that the regulation was enforceable, a provision, similar to that in section 135AB of the *National Health Act 1953*, could prescribe that a breach of the privacy provisions of the Exposure Bill constitute an interference with the privacy of an individual for the purposes of section 13 of the Privacy Act.

[9] See, respectively, Part IIIA of the Privacy Act, section 135AA of the *National Health Act 1953* and Division 4 of the Privacy Act.

(b) The Exposure Bill could introduce amendments to the Privacy Act so that AML/CTF privacy regulation was located in the Privacy Act.

(c) Privacy provisions could be introduced by way of an enforceable AML/CTF Rule under section 191 of the Exposure Bill.

(d) Regulations could be made under section 6E of the Privacy Act to the effect that small business operators (or their prescribed acts or practices) for the purposes of the AML/CTF legislation were treated as if they were an "organisation" for the purposes of Privacy Act.

39. An approach introducing uniform privacy obligations on all reporting entities would also seem consistent with Australian Government's *Policy Principles for Anti-money laundering reform* document, which nominates "consistent regulation" as a key principle.[10]

Retention periods

40. The Exposure Bill invites comment on the appropriate minimum retention periods for information collected by reporting entities under Part 10. While any period may be arbitrary, it seems useful for the period to be determined with reference to the policy intent of NPP 4.2. This principle requires that personal information be destroyed once it is no longer needed for any purpose for which the information may be used or disclosed under NPP 2.

41. Such an approach highlights that a specific and clearly justified purpose must be articulated as to why the personal information is being retained.

Access to AUSTRAC-held data

42. The practice of collecting personal information for one purpose, for example, law enforcement, while allowing others to have access to that personal information for other, possibly unrelated, purposes goes against ordinary privacy principles. This is especially the case where adequate steps are not taken to ensure that the individual is reasonably aware of the further uses of their personal information, or where the individual has little or no choice in providing such information.

43. Under the FTR Act, AUSTRAC may grant access to individual personal information to nominated agencies. The policy settings underpinning the existing personal information sharing arrangements involving AUSTRAC and other agencies are intended to limit access to AUSTRAC data to those agencies that require it to address the objects of the legislation, notably to prevent or cease tax evasion and money laundering.

44. Division 4 of Part 11 of the Exposure Bill sets out the provisions relating to access to AUSTRAC data. The Office understands that it is intended that

10 http://www.ag.gov.au/agd/WWW/rwpattach.nsf/personal/7D725051B1171EE2CA256EAF00015A89/$FILE/Policy+0+Principles+Paper+for+Anti-Money+Laundering+reform.PDF

a range of Australian, State and Territory agencies, such as Centrelink, Child Support Agency and respective state and territory revenue collection bodies, will retain their existing ability to access personal financial information held by AUSTRAC under the provisions of the Exposure Bill. Moreover, it will be for AUSTRAC to decide which other agencies, subject to Division 4, will be permitted to have access to personal information it retains.

45. The Office submits that the replacement of the FTR Act with new legislation with its greater scope and impact does not, of itself, necessarily justify the continuance of the present data-sharing arrangements so as to permit access to the welfare and assistance agencies. In the event that the welfare and assistance agencies are to be given access to AUSTRAC data, then a statement of the legislative objects of the Exposure Bill should reflect an intention to allow such agencies to scrutinise the AUSTRAC data for their purposes. Accordingly, community consultation should be conducted expressly on this policy setting.

46. A number of factors support the need for careful review of access provisions to personal information held by AUSTRAC under the Exposure Bill, including:

- the likely increased volume and richness of personal data that will be available for collection by AUSTRAC and, hence, accessible by other agencies for purposes unrelated to anti-money laundering and counter-terrorism activities;
- the extent to which the community may be aware that personal information provided by individuals in the course of a wide range of financial and commercial transactions may be scrutinised by a number of government agencies; and
- the extent to which the exercise of the discretion reposed in AUSTRAC to make its data accessible to other agencies is a transparent and accountable process. In this context, the process to ensure transparency and accountability should be proportionate to the breadth of the scheme and the amount of data the designated agencies will have access to.

An alternative access regime

47. Section 99(1) of the Exposure Bill currently permits AUSTRAC to authorise, in writing,[11] other agencies to access AUSTRAC-held data for purposes of "performing that agency's functions or exercising its powers". The Office notes that agencies' functions and powers can often be defined in legislation in quite broad and general terms. Alternatively, it may be more appropriate for such purposes to be defined in greater specificity.

48. This section could be amended to a more privacy sensitive form by narrowing these purposes to those which are consistent with and relevant to the underlying policy intent of the AML/CTF regulatory scheme.

[11] The status of this authority is unclear, as it is not apparent what form of instrument the written authorisation is intended to be.

49. This section could also be usefully amended by requiring transparency (including through mandatory consultation) and oversight over how the authority is exercised (including by clarifying that the written authority made by AUSTRAC is subject to Parliamentary scrutiny and disallowance).

Threshold transactions

50. As noted earlier, currently in excess of 2 million reports to AUSTRAC are generated due to a transaction being in excess of the threshold figure for "significant transaction". This represents a significant volume of personal information.

51. The Office notes that the number of significant cash transaction reports has increased approximately 200% since 1991. For this category of reporting, the level of growth may suggest that consideration needs to be given as to whether the threshold figure of $10,000, which has remained constant since the scheme was introduced, remains the "significant amount" anticipated when the FTR Act was drafted.

52. If this figure remains at this current prescribed level, then, as a consequence of price inflation, the reporting scheme will increasingly capture personal information regarding transactions that may not have been anticipated when the legislation was first drafted.

53. Further, section 5 of the Exposure Bill defines 'threshold transaction' and introduces the authority for AUSTRAC to prescribe, by regulation, threshold transactions for specified transactions less than $10,000, including non-cash transactions. The Office understands that such regulations are those provided for by section 205 of the Exposure Bill and prescribed by the Governor-General.

54. The justification for requiring the need to prescribe what could be relatively small transactions as threshold transactions requiring the collection and reporting of personal information is not clear. Further, it may be useful for the regulation provision to contain a consultation requirement.