CHAPTER 4

PRIVACY CONCERNS

4.1 The Office of the Privacy Commissioner (OPC), the Australian Privacy Foundation (APF), the Office of the NSW Privacy Commissioner (NSWPC), the NSW Council for Civil Liberties (NSWCCL) and Liberty Victoria provided the committee with a non-industry perspective on the possible impact of the proposed AML/CTF regime on the privacy and civil liberties rights of individuals.[1]

4.2 In particular, the concerns raised by these organisations related to:

- the lack of consultation on privacy issues prior to the release of the Exposure Bill;
- the need for a privacy impact assessment for the Exposure Bill;
- the wide range of entities collecting information under the regime;
- the type and extent of information to be collected under the regime;
- use of information collected pursuant to the regime; and
- the application of the *Privacy Act 1988* (Privacy Act).

Consultation on privacy issues

4.3 As noted in Chapter 3, the proposed AML/CTF regime has been developed since January 2004 in consultation between government and industry groups. NSWCCL and the APF both raised concerns that, despite this lengthy consultation period, privacy and civil liberties groups and consumer representatives were not given the opportunity to be involved in the drafting of the legislation until after the release of the Exposure Bill.[2] Ms Anna Johnson of the APF also stated that there was a lack of transparency to the process, citing the Department's reluctance to make available submissions received during public consultations in 2004.[3]

4.4 In evidence to the committee, the Department stated that while consumer advocate and privacy groups are not involved in the ministerial advisory group, parallel discussions are occurring with these organisations. It is proposed that these consultations will take the form of an ongoing body which will meet quarterly; and it is anticipated that the Minister would attend one or two of those meetings.[4]

---

1 See Australian Privacy Foundation, *Submission 4*; Office of the NSW Privacy Commissioner, *Submission 5*; NSW Council for Civil Liberties, *Submission 10*; Office of the Privacy Commissioner, *Submission 23*.

2 *Submission 4*, p. 2; *Submission 10*, p. 3.

3 *Committee Hansard*, 14 March 2006, p. 31.

4 *Committee Hansard*, 14 March 2006, p. 64.

4.5 AUSTRAC also confirmed that the Department and AUSTRAC have been involved in discussions with privacy, civil liberties and consumer groups, and that issues about coverage of the Privacy Act are being dealt with between the OPC and the Department. Further:

> All matters raised during the consultation period, including in submissions to this Committee, will be taken into account in reviewing the drafting of the Bill and the Rules. AUSTRAC is consulting with the Privacy Commissioner's office on the draft Rules and on guidance which will underlie the Rules, both directly and through its Privacy Consultative Committee, which also includes privacy, civil liberties and consumer groups.[5]

Privacy impact assessment

4.6 The committee's attention was directed to the issue of whether the potentially invasive measures in the Exposure Bill are necessary and proportionate to the risks they are meant to address; namely, money laundering and financing terrorism. [6]

4.7 To address this concern, the OPC suggested that a Privacy Impact Assessment (PIA) be performed for the legislation. The OPC described a PIA as:

> … an assessment tool that describes, in detail, the personal information flows in a project, and analyses the possible 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.[7]

4.8 The OPC indicated that it had previously recommended to the Department that a PIA be conducted on the legislation:

> The Office provided comments to the Criminal Justice Division (CJD) of the Attorney-General's Department on a draft of the *Anti-Money Laundering Bill* 2004 on 14 January 2005. In these comments the Office suggested that at the end of the second round of consultations, it would be useful for the CJD to conduct a Privacy Impact Assessment (PIA) regarding the next version of the Bill.
>
> The Office believes that PIAs are a good practice approach to assessing the privacy risks associated with projects that have complex information flows.
>
> … Accordingly, I anticipate that the Office will again recommend to the Attorney-General's Department as part of our response to their request for comments on the Exposure Draft that they should consider undertaking a PIA.[8]

---

5 *Submission 33*, p. 3.

6 See, for example, *Submission 4*, p. 3; *Submission 23*, p. 7.

7 *Submission 23*, pp 7-8.

8 *Submission 23A*, p. 1.

4.9 In evidence to the committee, Mr David Vaile of the APF also indicated its support for a PIA.[9] Mr Stephen Blanks of the CCL supported both a PIA and a human rights impact assessment for the Exposure Bill.[10]

4.10 The Department indicated to the committee that, at this stage, the Minister has not agreed to a PIA being conducted for the Exposure Bill.[11]

4.11 In view of the far-ranging nature of the provisions contained in the Exposure Bill, the committee is of the view that a PIA would be beneficial.

Range of entities collecting information

4.12 The APF pointed out that there has been no attempt to quantify the number of entities expected to be captured by the various types of services listed in section 6 of the Exposure Bill.[12] This makes it difficult to ascertain the extent to which some reporting entities will be covered by the National Privacy Principles (NPPs) in the Privacy Act. However, what is known, is that:

> … [i]f 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.[13]

4.13 A number of submissions also raised concerns about the use of reporting entities for performing security surveillance. Mr Luke Lawler from the Credit Union Industry Association (CUIA) described the situation as follows:

> There is a kind of deputisation of the entire financial sector to gather information on people and report information on people to a vast number of federal agencies.

4.14 NSWCCL described the regime as 'drastically reducing' the extent to which government and government agencies will be accountable for Australia's national security and intelligence regime.[14]

Type and extent of information to be collected under the regime

4.15 Submissions and witnesses raised concerns with respect to the wide range of information to be collected by reporting entities under the regime.

---

9 *Committee Hansard*, 14 March 2006, p. 34.

10 *Committee Hansard*, 14 March 2006, p. 37.

11 *Committee Hansard*, 14 March 2006, p. 69.

12 *Submission 4*, p. 5.

13 OPC, *Submission 23*, p. 3.

14 *Submission 10*, p. 8.

Customer identification information

4.16 The APF considered that the customer identification procedures in Part 2 of the Exposure Bill are contrary to the principle of anonymity provided for in NPP 8; that is, wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.[15] The APF was particularly concerned at the effect on individuals' ability to search for an acceptable financial advisor without identifying themselves.[16]

4.17 Mr Raj Venga of the Australian Association of Permanent Building Societies also argued against aspects of the identification process, anticipating that they would be regarded by customers as overly intrusive:

> We do not believe that the government and its agencies have properly considered how intrusive the customer identification and monitoring requirements of the bill and rules actually are. We see such intrusion as a bad thing. The fact of the matter is that the overwhelming majority of our members—almost all of them—are neither money launderers nor terrorists. Customers will not welcome the prospect of providing ID information—although they do it now on a limited basis—or responding to queries in relation to the source of funds, income and financial assets or their financial situation. These are personal and confidential matters that customers would understandably not wish to share, unless absolutely necessary in relation to the designated service—for example, applying for a loan. If a customer chooses not to cooperate, do we terminate our business relationship with the customer? And are we required to lodge a suspect matter report on the basis that the customer has not been forthcoming in providing this information?[17]

4.18 American Express considered that the scope of the minimum customer information required under the Rules is unnecessarily wide:

> For the purpose of issuing a relatively low risk product such as a credit card, it is of no business value to record: place of birth, nationality or country of residence. Verifying these particulars would be disproportionately costly and labour intensive and would yield no information of regulatory value for AML/CTF purposes. In addition, such information of necessity becomes a surrogate for identifying ethnicity, which in turn may lead to inappropriate assumptions being used as a basis for decision-making. The legitimate objectives of privacy and anti-discrimination laws may thus be undermined.[18]

4.19 In response to this comment, the Department and AUSTRAC pointed out that American Express' concerns appeared to be directed to a draft version of the customer

---

15 See, for example, *Submission 5*, pp 2-3; *Submission 23*, p. 6.

16 *Submission 4*, p. 5.

17 *Committee Hansard*, 14 March 2006, p. 4.

18 *Submission 15*, p. 4.

identification Rules, which had included a list of specific prescribed requirements. The Department indicated that these Rules would be redrafted to reflect a more risk-based approach. [19]

4.20 In an answer to a question on notice, AUSTRAC confirmed that the policy in relation to customer identification has changed since the committee's hearing:

> The Bill will be redrafted to provide for customer identification programs, to be developed by reporting entities, which take into account the level of risk in determining what identification process is to be applied to particular customers. Draft Rules have been prepared reflecting this change. Those Rules are currently with industry working groups but will be made more widely available after industry's views have been received. This will include discussions with the Privacy Commissioner's office.[20]

AML/CTF Programs

4.21 The AML/CTF Program requirements also triggered concerns from a privacy perspective; namely, the volume and type of information being provided to reporting entities under the customer due diligence requirements in the AML/CTF Program Rules.

4.22 The APF stated that reducing the risk of money-laundering and counter terrorism should not require monitoring of all customers and all transactions. The APF submitted that the 'floor' for the minimum 'Know Your Customer' information is set too low and the additional 'Know Your Customer' information and enhanced due diligence requirements are likely to apply to too many customers.[21]

4.23 The APF acknowledged that there was provision for full or partial exemption from identification procedures for some low-risk services. However, in its view, the drafting of such exemptions should not be 'left to the discretion and judgement of AUSTRAC to make in Rules'.[22]

4.24 Further, privacy implications are likely to arise from the requirement that reporting entities assign customers a risk classification.[23] The APF and the NSWPC noted that an assessment that a customer is 'higher risk' will potentially have an adverse affect on the customer, and the Exposure Bill lacks a review mechanism for a customer to challenge the risk assessment.[24]

---

19 *Committee Hansard*, 14 March 2006, p. 70.

20 *Submission 33*, p. 3.

21 *Submission 4*, p. 8.

22 *Submission 4*, p. 6.

23 *Submission 5*, p. 2

24 *Submission 4*, p. 8.

Impact of extensive 'suspicious matters' reporting obligations

4.25 Part 3 of the Exposure Bill provides that reporting entities must report certain 'suspicious matters' and transactions to AUSTRAC. 'Suspicious matters' is not defined in the Exposure Bill. The matters to be taken into account in determining whether there are reasonable grounds to report a suspicious matter will be set out in the Rules. Proposed subsection 39(4) makes it an offence if reporting entities fail to notify AUSTRAC of suspicious matters.

4.26 Five issues were raised in submissions and in evidence to the committee, regarding the obligation on reporting entities to report suspicious matters:

- the lack of precision in the definition of suspicious matters, particularly that the matters are not necessarily restricted to reports regarding money-laundering or terrorist financing;
- the probability of over-reporting of suspicious matters by reporting entities to avoid prosecution;
- the potentially discriminatory impacts of the reporting obligation;
- the lack of notice and openness in relation to the reporting regime, given that there is no requirement that reporting entities inform their clients that a suspicious matter report has been made to AUSTRAC; and
- the potentially conflicting obligations of employees of reporting entities to make suspicious matter reports, but not to tip off customers.[25]

4.27 The APF argued that the whole concept of reporting 'suspicions' by employees of reporting entities who are not qualified and trained investigators is inherently flawed:

> The criteria suggested in AUSTRAC guidance on suspect transaction reporting have always been highly subjective. The draft AML/CTF Rules and Guidelines for suspicious matter reporting which accompany the draft Bill are no better. They include appearance and behavioural factors as well as supposedly factual matters which there is no reason for employees of reporting entities to know.[26]

4.28 The APF argued further that the result of such broad and subjective guidance, and of the penalties for failure to report, would be either:

> • Even greater intrusion into customers' personal affairs, often based on 'guesswork', and/or,

25 See *Submission 4*, pp 6-7; *Submission 10*, pp 6-8; *Submission 23*, p. 4; *Submission 26*, pp 8-11; *Committee Hansard*, 14 March 2006, pp 20, 24-25, and 57.

26 *Submission 4*, pp 6-7.

> • Over-reporting because of an absence of information – 'to be on the safe side'.[27]

4.29 NSWCCL highlighted the potential impact of the obligation to report suspicious matters with other elements of the Exposure Bill:

> Part 9 (Countermeasures) of the proposed legislation allow the government to prohibit financial transaction to and from residents of particular countries. The combined effect of these provisions could be to encourage unwarranted 'suspicion' against persons of particular ethnic backgrounds or appearances. If so, this may create discrimination against individuals from non English-speaking backgrounds, because their behaviour, language, and lack of familiarity with Australian institutions and laws could lead to false 'suspicions [matter]' reports against them.[28]

4.30 In response to arguments suggesting 'racial profiling' may be a consequence of the suspicious matters reporting requirements, the Department had the following comments:

> If a person's appearance and behaviour give rise to suspicion on the part of the bank then there would be an obligation to report. I do not see how we can write into the legislation 'as long as you don't form that suspicion on a racist basis'. I think there are limits to what the legislation can do. If we decide that we want suspicions reported then some suspicions will be reported, if people do it properly. Some of those suspicions will be groundless and some will be based on things they should not base suspicions on.[29]

4.31 When asked about the training of staff to report suspicious matters and transactions, the Department said:

> I suggest that in relation to the question on how you are going to train staff to recognise risks and so on, there is at least an attempt in this bill to ensure that the programs require that sort of training for staff, whereas if you look at the existing FTR Act there is just the broad obligation. We recognise that experience will build over time and that at least there is an attempt to build a platform.[30]

4.32 The OPC noted that the reporting obligation in proposed section 39 goes beyond the reporting of information in relation to money-laundering and terrorism offences themselves.[31] Liberty Victoria highlighted that the obligation extends even

---

27 *Submission 4*, pp 6-7.

28 *Submission 10*, p. 8.

29 *Committee Hansard*, 14 March 2006, p. 70.

30 *Committee Hansard*, 14 March 2006, p. 63.

31 *Submission 23*, p. 4.

beyond information which might be relevant to serious offences, to encompass *any* offence – state or federal, and offences against foreign laws.[32]

4.33 Mr Luke Lawler of the CUIA told the committee of the experience in the US when similar legislation was introduced:

> One of the lessons from the experience of the United States is on the sheer number of reports being filed. There was an incredible increase in the number of suspicious activity reports that were being filed, so the financial intelligence unit over there was flooded with these reports with personal information about individuals, to the point where they were trying to advise industry to ease off a bit and be a bit more selective about the kinds of reports they were lodging. But industry was concerned because there were some high profile cases where some regulated entities were hit with very big fines for having inadequate anti-money laundering regimes. So in order to avoid any prospect of being prosecuted, they were pumping out these suspicious activity reports.[33]

4.34 Similarly, Ms Rhonda Luo of the NSWCCL told the committee that there was no utility in a system which generates over-reporting:

> Over-reporting is also very likely to result in misinformation being collected against individuals. If the object of the legislation is to identify and prevent international financial crimes, there is simply no use in having a large volume of possibly useless and wrong information against our citizens. It is possible that many innocent people will be caught up in these measures. More experienced, if I may say that, money launderers and financiers will be more likely to escape the simple pitfalls in the legislation.[34]

4.35 To rectify some of these problems, NSWCCL suggested that there be provision in the Exposure Bill for:

- notification to be given to customers at the beginning of a business relationship that business and service providers are required to report their financial activities that are regarded as 'suspicious';
- ex post facto notice to be given to individuals that a suspicious matter report has been made; and
- mechanisms by which individuals may be warned against financial products or transactions that are likely to generate a suspicious matter report.[35]

4.36 The Department justified the suspicious matters reporting requirements on several grounds. In its view, the legislation builds on what is already in the FTR Act,

---

32 *Submission 26*, p. 10.

33 *Committee Hansard*, 14 March 2006, p. 11.

34 *Committee Hansard*, 14 March 2006, p. 39.

35 *Submission 10*, pp 6-7.

since the key parts of the reporting requirement provisions are taken word for word from the existing Act:

> Those provisions have been there since 1988 and the number of suspicious transaction reports has gradually risen during that period from a fairly low level to the level that it is now at. They have never produced the sorts of problems which people are now saying that these provisions will produce.[36]

4.37 Further:

> In relation to the privacy issues, I hear what they say… But I do not know that there is a solution to some of the issues that they have raised. But what we then expect of the entity is that essentially they forget that they have put in a suspect transaction report, because it becomes the responsibility of AUSTRAC and the law enforcement agencies to decide whether to take action. We do not want reporting entities to be keeping records and blacklists of people who have put in suspicious transaction reports. [37]

Secrecy and access

4.38 The privacy implications of the wide collection requirements outlined above are compounded by the secrecy provisions in Part 11 of the Exposure Bill and, in particular, their application to suspicious matters reporting.

4.39 Ms Anna Johnson of the APF made the following comment on the provisions:

> We reserve our strongest criticism for the notion of secret reporting of suspicious matters. In our view, the concept of secret files compiled on the basis of amateur assessments and wholly subjective criteria is inconsistent with a free society.[38]

4.40 Having noted that the information in suspicious matter reports could be of 'dubious quality', because the reports are based on the subjective judgement of the employees of reporting entities, NSWCCL went on to say:

> … [t]he proposed regime also offends against individuals' access and correction rights under privacy laws, as the privacy-exempt suspicious transactions list thus created will be exempt from [Freedom of Information] law. It is uncertain how AUSTRAC will deal with information that appears to be unreliable, but it is submitted that the object of the legislation – prevention of terrorist financing – cannot be met if government or international investigations proceed on unreliable information. CCL notes that these secrecy provisions go beyond any existing regime in Australia, and even beyond the controversial wire-tapping laws in the United States.[39]

---

36 *Committee Hansard*, 14 March 2006, p. 62.

37 *Committee Hansard*, 14 March 2006, pp 62-63.

38 *Committee Hansard*, 14 March 2006, p. 30.

39 *Submission 10*, p. 6.

4.41 NSWCCL also suggested that there should be a notification given to customers at the beginning of a business relationship that business and service providers are required to monitor their financial activities.[40]

4.42 Representatives from the Department and AUSTRAC responded to the concerns with respect to secrecy as follows:

> The only tipping-off provisions in here are if you have put in a suspicious transaction report, you are not allowed to tell people that you have put in the report.
>
> … [T]here will be nothing at law stopping them from saying, if they wanted to, 'We consider you to be a high risk.' All they are not allowed to disclose is if in fact something has triggered an actual suspicion rather than a view that the customer is high risk. Somebody can be a high risk customer and never raise a suspicion, because even though they are high risk, their business is completely legitimate. It is only about putting in the suspicious matter report that the tipping off provision applies. If a customer comes to bank or a casino under privacy laws and asks whether they have been classified as high risk, I do not see that there is any way they can refuse to tell them.[41]

Need for public education campaign

4.43 The committee heard that there is a need for a public education campaign about the implications of the new regime. For example, Mr Luke Lawler of the CUIA told the committee that he anticipated that credit union customers would not react positively to a number of elements of the regime:

> Credit unions and other regulated entities will be required to collect baseline information on all customers. They will have to give all customers a risk classification, they will have to identify customers and services that pose a high risk, and they will have to collect quite detailed information on some customers and carry out transaction monitoring. Regulated entities will be obliged to report suspicious matters, even in cases where there is no actual transaction. Because of the impact on customers of these proposals, we have said from the outset that a significant public education campaign will be needed to explain why your financial institution will be asking you for more information about your personal affairs. We think this will come as a shock and a surprise to a lot of customers.[42]

4.44 Mr Lawler emphasised that such a public awareness campaign should inform customers that the actions taken by reporting entities are due to legislative requirements and are not being taken merely of their own volition:

---

40 *Submission 10*, p. 7.

41 *Committee Hansard*, 14 March 2006, p. 71.

42 *Committee Hansard*, 14 March 2006, p. 5.

> We would anticipate that, depending on the extent to which one has to gather this sort of additional information on customers beyond what is gathered in the ordinary course of business now, many of our members would be quite affronted and quite surprised at being asked to provide this sort of information. Even some of the baseline information that is proposed to be provided includes, for example, place of birth. If you provide a birth certificate as ID, that is all taken care of but if you provide, for example, a drivers licence as ID, you are not necessarily disclosing your place of birth. Nevertheless, the regulated entity will have to ask you for your place of birth. Some people might find that unnecessary and a little creepy…
>
> [W]e will be quite keen to explain that if we have to collect this sort of information—and in cases where someone fits a profile of possibly a high risk or a high-risk product, we will have to go and get some more information on them—we will want them to be aware that this is a legislative requirement and that we are not doing this simply to intrude in their personal affairs.[43]

4.45 The Department noted that it had considered the need for an awareness campaign to inform the public that these obligations stemmed from government and not from industry. The Department has given a commitment that such a campaign will take place, although the appropriate time for such a campaign remains to be determined.[44]

Use of information

4.46 Not only does the Exposure Bill provide for the collection of a great deal of additional material, it would also permit the use of that information for a wide range of purposes that arguably go beyond the objectives of the legislation. This has obvious privacy implications.

4.47 This issue has two elements: the first is the uses permitted by reporting entities of information collected from their customers; the second is the extent of AUSTRAC's authority to disseminate information contained in its system to other agencies.

Use of information for secondary purposes

4.48 Some submissions and evidence drew to the committee's attention the issue of use by reporting entities of information collected under the regime for secondary purposes. This matter is particularly relevant to those reporting entities not bound by the NPPs (discussed below).

4.49 As an example of the potential misuse of this information, Ms Anna Johnson of the APF drew the committee's attention to a recent article in the Law Society

---

43 *Committee Hansard*, 14 March 2006, pp 8-9.

44 *Committee Hansard*, 14 March 2006, p. 73.

Journal that promoted the benefits of the Exposure Bill as a way of generating further business because reporting entities will be required to know more about their customers' finances.[45] The article pointed out that the Exposure Bill would allow lawyers to have 'at their fingertips' information that would effectively allow them to sell a raft of additional services to their customers.[46]

4.50 This article raised the concern that reporting entities could use the proposed legislative requirements to compulsorily collect a wide range of personal customer information and use it for the general purposes of marketing and profiling.

Access to AUSTRAC-held data

4.51 Division 4 of Part 11 of the Exposure Bill provides for government agencies to access information held by AUSTRAC. In particular, proposed section 99 provides for AUSTRAC to grant access to 'designated agencies' 'for the purposes of performing the agency's functions and exercising the agency's powers';[47] that is, for purposes that may be completely unrelated to AML or CTF. Designated agencies are defined in proposed section 5, and include not only law enforcement agencies such as the Australian Federal Police, but also a wider group of agencies including the Child Support Agency and Centrelink. Further provision is also made to disseminate information to 'an authority of agency of a State or Territory, where the authority or agency is specified in the regulations'.[48]

4.52 The scope of the information dissemination by AUSTRAC pursuant to this provision raised some concerns. The OPC understood that the intention is that agencies with current access to AUSTRAC data under the FTR Act would retain that access, and it will be up to AUSTRAC to decide if other agencies are able to access information collected under the Exposure Bill.[49] The OPC's view on such an arrangement was 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.

45 *Committee Hansard*, 14 March 2006, p. 30.

46 See further, Professor John Broome, as quoted in J. Lewis, 'Cleaning up: Anti-money laundering laws need not spell disaster', *Law Society Journal*, March 2006, p. 22.

47 See, for example, *Submission 4*, p. 10; *Submission 10*, p. 5; *Submission 23*, pp 9-11.

48 Proposed section 5.

49 *Submission 23*, pp 9-10.

> Accordingly, community consultation should be conducted expressly on this policy setting.[50]

4.53 The OPC suggested that proposed section 99 be amended 'to a more privacy sensitive form' in which access to AUSTRAC-held data is restricted to purposes consistent with and relevant to the underlying purpose of the AML/CTF scheme.[51]

4.54 A representative of AUSTRAC clarified the scope of the information-sharing provisions of the Exposure Bill:

> … section 99(1) of the bill allows AUSTRAC to authorise specified officials of specified designated agencies. It does not allow us to decide which agencies may have access. The designated agencies are those agencies listed in section 5 under the definition. That provision is about what we do now, which is not specifically set out in our Act. In our MOUs with our partner agencies, we actually specify a limited number of officers who have access to our information. This is a provision that legislatively for the future will require us to specify them. So it is not like AUSTRAC can say, 'These are more agencies, other than are on the face of the bill, that can have access to our information.'

4.55 On the issue of the purposes for which designated agencies could access AUSTRAC-held data, representatives of AUSTRAC and the Department said:

> Some of this comes back to the questions about the definition of money laundering and the fact that the predicate offences for money laundering are extremely broad … [S]ome of those issues are matters of government policy about who should have access to our information and for what purposes.

4.56 In an answer to a question on notice, AUSTRAC noted that FTR information currently available to designated agencies is used to combat money laundering:

> The FTR information available to the designated agencies assists them to stop illegal conduct which would otherwise result in the laundering of money. If the agencies were not able to use the information to identify and prosecute offenders for predicate offences, where money laundering has not occurred because of the timing of the identification and investigation of the predicate offence, then the success of Australia's very effective anti-money laundering program would be severely diminished.[52]

4.57 The Department also noted specifically in relation to tax that the close relationship between tax, tax evasion and money laundering, and the fact that the taxation power underpins the FTR Act, makes it appropriate for the ATO to have

---

50 *Submission 23*, pp 9-10.

51 *Submission 23*, p. 10.

52 *Submission 33*, p. 3.

access. The Department undertook to consider the other comments in relation to which matters should be made explicit in the objects clause.[53]

Application of the Privacy Act

4.58 An important consideration in assessing the privacy implications of the Exposure Bill is the extent to which protections afforded by the Privacy Act apply to both AUSTRAC and government agencies, and the various service providers that would become reporting entities under the Exposure Bill.

AUSTRAC

4.59 A number of submissions noted that the Exposure Bill does make provision for AUSTRAC to obtain assurances from state, territory and foreign agencies about compliance with the Information Privacy Principles (IPPs) in the Privacy Act. However, the submissions questioned the enforceability of such assurances and what remedies individuals may have in the event that their privacy is interfered with.[54]

4.60 In response, AUSTRAC indicated to the committee that:

> … the memoranda of understanding that we currently have with our state and territory partner agencies actually state that they undertake to comply with the information privacy principles.[55]

Application of the National Privacy Principles to reporting entities

4.61 The NPPs in the Privacy Act regulate the collection, use and disclosure and handling of personal information by private sector 'organisations'. Reporting entities that are 'organisations' for the purposes of the Privacy Act will be required to comply with the NPPs.

4.62 The OPC outlined its concern that many of the privacy protections offered in the NPPs, such as the obligations in relation to data quality, notice and openness, will only apply to reporting entities to the extent that they are 'organisations' – as defined in the Privacy Act.[56]

4.63 Of particular concern is the fact that 'small businesses' – that is, businesses with an annual turnover of $3 million or less – are generally exempt from the NPPs.[57] NSWPC had the following comment in this regard:

---

53 *Committee Hansard*, 14 March 2006, p. 81.

54 See, for example, *Submission 4*, p. 10; *Submission 23*, p. 8.

55 *Committee Hansard*, 14 March 2006, p. 81.

56 *Submission 23*, pp 5-6.

57 See section 6D of the *Privacy Act 1988*; *Submission 23*, p. 5.

> It is out experience that many small businesses are either not very familiar with best privacy practice or choose not to follow it for a variety of reasons, predominantly because they do not have an obligation under the law to protect personal information of individuals. We receive a steady stream of complaints from members of the public alleging privacy breaches by medium and small businesses of the like that are likely to become reporting entities under the Bill. Unfortunately, under the current legislative regime neither state nor federal privacy agencies have effective powers to deal with such complaints.[58]

4.64 Witnesses before the committee demonstrate the mixed extent to which the NPPs might apply to reporting entities:

- All members of the Credit Union Industry Association are subject to the NPPs, because even those members to whom the NPPs did not apply had opted into the regime.[59] This is probably also the case for members of the Australian Association of Permanent Building Societies.[60]
- Some members of the Institute of Chartered Accountants in Australia are subject to the NPPs but not all.[61]
- Most members of the Financial Planning Association of Australia are subject to the NPPs, either because they are required to under the Privacy Act, or they had opted into the regime.[62]

4.65 The OPC, the NSWPC, and the APF all recommended that, given the personal and sensitive nature of the information being handled, all reporting entities should have privacy obligations imposed on them that are at least equal to the requirements of the NPPs.[63] The APF went further in suggesting that the Exposure Bill should be amended to specifically remove from reporting entities any exemption they may enjoy under the Privacy Act.[64]

4.66 The OPC also stated that the Exposure Bill should include additional privacy provisions which are consistent with the Privacy Act for all reporting entities, regardless of size or type.[65] The OPC made the following suggestions as to how this could be achieved:

---

58 *Submission 5*, p. 1.

59 *Committee Hansard*, 14 March 2006, p. 9

60 *Committee Hansard*, 14 March 2006, p. 9.

61 *Committee Hansard*, 14 March 2006, p. 46.

62 *Committee Hansard*, 14 March 2006, p. 21.

63 *Submission 23*, p. 5; *Submission 5*, p. 1; *Submission 4*, p. 13.

64 *Submission 4*, p. 13.

65 *Submission 23*, p. 8.

- Through privacy protections set out in a Schedule to the Exposure Bill, with an enforcement provision to the effect that a breach of the protection measures constitutes interference with the privacy of an individual for the purposes of section 13 of the Privacy Act.
- Amending the Privacy Act to specifically incorporate privacy with respect to AML/CTF.
- Including privacy provisions by way of an enforceable rule under section 191 of the Exposure Bill.
- Regulations under section 6E of the Privacy Act to include small businesses as 'organisations' for the purposes of the AML/CTF legislation.[66]

4.67 In the course of the public hearing, the Department acknowledged that the issue of the small business exemption to the NPPs was an issue that the Federal Government would have to, and will, address.[67]

Retention of information

4.68 An associated issue is the rules regulating the retention of information gathered by reporting agencies pursuant to the proposed regime. Part 10 of the Exposure Bill sets out the record-keeping requirements for reporting entities, and public comment has been invited on the duration of retention periods for records and documents.

4.69 The OPC considered that, while any period may be arbitrary, some guidance could be taken from the NPPs, which provides for the destruction of that personal information once it is no longer needed for any purpose for which the information may be used or disclosed. In the OPC's view such an approach highlights that there must be a 'specific and clearly justified' purpose for the retention of personal information.[68]

4.70 The APF also referred to the NPPs, and stated that the retention period should be for the shortest period possible to fulfil the objectives of the legislation. The APF noted that while there may be a temptation to set long or indefinite retention periods on the basis of a hypothetical utility, this should be resisted, particularly for suspicious matter reports which are 'hidden' from the subject.[69]

4.71 In considering the period for retention, Liberty Victoria suggested a period of five years, stating that anything outside of that time frame is:

---

66 *Submission 23*, pp 8-9.

67 *Committee Hansard*, 14 March 2006, p. 82.

68 *Submission 23*, p. 9, referring specifically to NPP 4.2.

69 *Submission 4*, p. 9.

> … likely to be of limited value in money laundering or terrorism offences which are far more likely to occur contemporaneously with the transaction.[70]

Committee view

4.72 Despite expressing optimism in the previous chapter that the majority of outstanding issues will be resolved before finalisation of the regime, the committee does remain concerned about the apparent lack of formal consultation with privacy, civil rights and consumer representative groups in the development of the regime to this point. The committee is of the view that this may have resulted in some fundamental privacy, consumer and civil rights issues being overlooked. Nevertheless, the committee is also hopeful that these issues will be addressed through the parallel discussion groups established by the Department.

4.73 The committee notes the OPC's suggestion that an independent PIA would be useful in relation to the Exposure Bill. **The committee agrees with this view and believes that a PIA would be beneficial in achieving a more balanced approach to the AML/CTF regime**. This is particularly important given the complexity of the Exposure Bill, the vast number of reporting entities and transactions covered by the Exposure Bill's operation, the amount and type of information to be collected, and the ability of various agencies to access that information. **The committee therefore strongly suggests that such an assessment be conducted**.

4.74 The committee also notes that the Federal Government intends to address the issue of the small business exemption to the NPPs in relation to reporting entities. However, the committee believes that the concerns raised in submissions and evidence highlight a larger problem in relation to the privacy obligations of reporting entities. The committee's view is that any PIA should include a review as to whether the privacy protections set out in the NPPs are sufficient for the purposes of the information being collected and handled by reporting entities.

4.75 If it is found that the privacy protections in the NPPs are not sufficient for the purposes of reporting entities, then adequate privacy protections could usefully be included in the AML/CTF legislative package. If the privacy protections in the NPPs are considered adequate for the purposes of reporting entities, then the Federal Government should ensure that all reporting entities are made subject to privacy obligations equivalent to those contained in the NPPs.

4.76 In line with a further suggestion by the OPC, **the committee also considers that the Exposure Bill should contain a clear objective statement that is reflective of the intention to allow federal, state and territory agencies, including welfare and support agencies, to access and utilise AUSTRAC data for their own purposes – purposes which may not be related in any way to AML or CTF**.

---

70 *Submission 26*, p. 14.

4.77 The committee considers that such a statement should be included in the final version of the bill to make it clear at the outset that this may occur.

Senator Marise Payne
Committee Chair