CHAPTER 4

PRIVACY AND DISCRIMINATION CONCERNS

Introduction

4.1 The committee suggested in its report on the Exposure Bill that a Privacy Impact Assessment of the proposed legislation should be conducted. The committee is pleased to note that the Department has obtained such an assessment. However, some issues relating to privacy and discrimination remain a concern for stakeholders. In particular, witnesses expressed concern that the Bill may lead to discrimination by financial institutions based on race, religion, nationality or ethnic origin.

4.2 The privacy and discrimination issues raised by witnesses related to provisions in the Bill regarding:

- customer identification;
- customer verification;
- customer due diligence;
- the collection and storage of personal and sensitive information;
- the sharing of AUSTRAC held information with various agencies;
- the reporting of suspicious matters; and
- the performance of money-laundering and terrorism financing risk-assessments.

Discrimination

Risk-based approach

4.3 Liberty Victoria considers that the existing risk-based approach to the regime will 'mean that reporting entities will have significant discretion in complying with their AML/CTF obligations. In particular, financial institutions have considerable discretion in constructing the risk profiles of their customers. This discretion carries a serious danger of discrimination based on race, religion and nationality'.[1]

4.4 Witnesses expressed concern regarding the ability of staff to appropriately perform risk assessments and in particular the level of training required to undertake intelligence assessments.

---

1 *Submission 1*, p.5. Also, see *Submission 32*, p.2.

> …under the *Financial Transactions Reports Act 1988* (Cth), one commentator has described the money-laundering related training provided by Australian financial institutions to their staff as 'lax'.[2]
>
> How can the Australian public be confident that the subjective nature of suspicious matter reports will not become even less reliable an indicator of wrong-doing once reporting obligations are extended to thousands of clerks and shop assistants who, despite the Bill's requirements and best intentions will never be able to be adequately trained for such a task?[3]

4.5 In relation to the issue of suspicious matter reporting, Liberty Victoria also drew attention to a Muslim religious obligation known as *zakat*, a type of charitable giving, and the process of non-bank remittance through the Islamic *hawala*.[4] The commercial model used to identify suspect funds classifies as 'suspect' an activity that makes little or no business sense. This creates a risk that religious activities may be characterised as a suspicious activity and result in a suspicious matter report.

Provision of immunity increases the risk of discrimination

4.6 Under clause 235 protection from liability is provided to a reporting entity, its officers, employees and agents from action or suit under any law 'in relation to anything done, or omitted to be done, in good faith' by a reporting entity 'in compliance, or in purported compliance' with provisions of the Act, regulations and AML/CTF rules. Liberty Victoria commented that conduct undertaken in 'good faith' may still breach anti-discrimination statutes and the provision of immunity increases the risk of discrimination and even sanctions discrimination.[5]

4.7 Liberty Victoria discussed the Explanatory Memorandum of the Bill which states that the provision of immunity under clause 235 is not intended to override the *Racial Discrimination Act 1975* (Cth) and stated 'if it is the intention of the government not to override the *Racial Discrimination Act 1975* then this should be expressly stated in the Bill'.[6]

4.8 The Department considered the concerns raised regarding clause 235 and responded:

> Clause 235…does not operate to displace the *Racial Discrimination Act 1975* (RDA). A person can only rely on the indemnity provided by clause 235…where they have acted in good faith. There is nothing in the AML/CTF Bill which permits or authorises compliance with the AML/CTF Bill to be met by actions which breach the RDA. The indemnity in clause

---

2 *Submission 1*, p.5.

3 *Submission 9*, p.6.

4 *Submission 1*, pp 6–7, p.15.

5 *Submission 1*, p.8. Also, see *Submission 32*, p.4.

6 *Submission 1*, p.8.

> 235 would not be available in circumstances where the reason for denial of service or disclosure was discriminatory or based on matters other than those properly encompassed by the object and operative provisions of the AML/CTF Bill.[7]

Secrecy undermines the rule of law

4.9 Another specific issue is that a concerned individual will not be fully aware of the collection, use and disclosure of personal information. The 'tipping off' provisions of the Bill ensure that a concerned individual will not normally be told that a suspicious matter report has been made to AUSTRAC, nor will that individual be told the reasons for the making of the report.

4.10 Liberty Victoria argued:

> It is the secrecy surrounding these flows of information that undermines the rule of law. Citizens subject to a Suspicious Matter report are not in a position to ensure that the 'reporting entity', AUSTRAC or other authorities in possession of his or her personal information are complying with the law. This is simply because s/he would not know such information has been communicated. The rule of law is put under even greater pressure when information flows onto foreign authorities where there are additional practical difficulties of monitoring the compliance of these foreign authorities with their undertakings.[8]

4.11 For this reason, Liberty Victoria supports a regular audit of the informational practices to ensure compliance with the law and suggests that the audit be conducted either by the Privacy Commissioner or the Human Rights and Equal Opportunities Commission (HREOC).

Privacy

Lack of consideration of privacy issues

4.12 The inquiry into the Exposure Bill revealed that privacy and civil liberty groups and consumer representatives had not been adequately consulted in relation to the Exposure Bill. The current inquiry has heard evidence in the same vein from stakeholder groups who believe that privacy issues are not being considered a priority.

4.13 The Australian Privacy Foundation (APF) commented on the failure of the Commonwealth Government to address privacy related issues and engage interested groups:

> During more than two years of consultation, the government has failed to significantly address the major privacy concerns drawn to its attention by

---

7 Attorney General's Department, answer to question on notice, 15 November 2006 (received 21 November 2006).

8 *Submission 1*, p.11.

> the APF, the Privacy Commissioner and other interested parties (and now it appears by the PIA).[9]

Type of and scope of information collected

Lack of customer anonymity

4.14 Clauses 139 and 140 of Part 12 (Offences) of the Bill concern the provision and receipt of a designated service using a false name or on the basis of customer anonymity. The APF comments that the provision of criminal offences in these circumstances 'hangs like a sword over anyone seeking to offer individuals simple advice, but also directly undermines the intent of National Privacy Principle 8 (anonymity)'.[10]

Information held on electoral rolls

4.15 Clause 13 of the Amending Bill makes consequential amendments to the *Electoral Act 1918* which allow bulk release of the joint Commonwealth and State electoral roll to reporting entities for the purposes of complying with their customer identification obligations.

4.16 The APF raised concerns on the ability to access information held on the electoral roll for identity verification and suggested that mechanisms be in place to ensure that this information is not used for secondary purposes (an entity's own business purpose). The APF commented:

> It is completely unrealistic, for example, to expect a bank which uses the electoral roll to establish that a customer has different name and/or address particulars not to also record that information in its customer database and use it for commercial purposes, including normal customer contact and marketing.[11]

4.17 Not all witnesses expressed concerns regarding the release of information held on electoral rolls. Some witnesses in their evidence requested an extension to the use of information held on electoral rolls. Baycorp suggested that access be extended to allow organisations, such as credit reporting agencies, which perform customer verification services to use this information to assist reporting entities in undertaking their customer due diligence obligations under the Bill.[12]

---

9 *Submission 9,* p.2.

10 *Submission 9,* p.3.

11 *Submission 9,* pp 8–9. Also, see *Submission 14,* p.4, *Submission 40a,* p.1.

12 *Committee Hansard*, 23 November 2006, pp 17–18. Also, see *Submission 15,* pp 2–3, *Submission 17,* p.2.

Population-wide surveillance of financial affairs

4.18 Privacy Victoria commented that the reporting obligations (including threshold amounts) in the Bill result in a significant risk of pervasive monitoring of the financial affairs of ordinary citizens. This monitoring would not necessarily be due to the suspect nature of transactions or the risk of money-laundering and terrorism financing. Ordinary citizens by virtue of engaging in everyday financial transaction such as wiring money overseas, purchasing a stored value card and taking a loan of $10,000 may be caught within these obligations.[13]

4.19 Privacy Victoria considered that addressing this potential of the reporting obligations to cover such a significant portion of the population should not occur by regulation. Privacy Victoria recommended that 'the scope of the measures should be set out in the legislation after due scrutiny and debate by Parliament, and be accompanied by safeguards that are proportionate to the measures that are to be enacted'.[14]

Requests to override Part IIIA of the Privacy Act

4.20 Many witnesses raised issues around the operation of the Bill and Part IIIA of the *Privacy Act 1988*. Witnesses expressed concerns that existing inconsistencies create uncertainty regarding the use of customer credit information for the purpose of the Bill, for example to assist in the customer verification process. Baycorp stated:

> An amendment to the current version of the Bill [is] required to make it expressly clear that credit information could be used for identity verification purposes. As the Act currently stands Part IIIA prohibits disclosure of credit information unless the information is contained in a credit report given to a credit provider who requested the report for the purposes of assessing an application for credit.[15]

4.21 The Office of the Privacy Commissioner (OPC) considered this matter and expressed caution that the AML/CTF Rules may allow for the disclosure of consumer credit reports in an expanded range of circumstances. OPC stated:

> The Office would be particularly concerned if this clause [Rules paragraph 2.2.14] intends to give reporting entities access to consumer credit reports where such access is currently prohibited by Part IIIA of the Privacy Act. Part IIIA restricts access to the consumer credit reporting system by providing prescriptive regulation and includes criminal sanctions for non-compliance, including fines of up to $150,000. The Office would caution against the Rules opening this system to reporting entities for purposes

13 *Submission 14,* pp 1–2. Also, see *Submission 40,* p.5.

14 *Submission 14,* p.2.

15 *Submission 22a,* p.4. Also, see *Submission 17,* p.2; *Submission 16a,* p.13.

> unrelated to consumer credit, unless such a measure is subject to careful consideration and clear justification.[16]

Access to AUSTRAC information

4.22 The Bill, under Division 4 (clauses 125 and 126), allows the Australian Taxation Office and approximately 30 different designated agencies to access information held by AUSTRAC. Under certain conditions, information can also be passed on to foreign authorities. The fact that such a broad range of agencies have access to AUSTRAC information concerned some stakeholders.[17]

4.23 Privacy Victoria raised the question of why it is necessary for agencies such as Centrelink and the Child Support Agency to have access to such sensitive information and why regulations are being used to authorise other State and Territory authorities and agencies to seek AUSTRAC data:

> Specifying the intended users and purposes for which the information is accessed would improve the transparency and enable Parliament to properly scrutinise and debate the appropriate scope and safeguards that should apply.[18]

Purpose of collection

4.24 Evidence received during the inquiry also expressed concern that AUSTRAC information, once accessed by designated agencies, may be used for secondary purposes which are unrelated to the initial purpose of collection, being the prevention of money-laundering and terrorism financing.[19]

4.25 The APF explained their concerns regarding designated agencies accessing AUSTRAC held information:

> There is no attempt to limit uses to AML-CTF investigations or even to investigation of other serious or organised crime. AUSTRAC information, misleadingly collected under the apparent justification of AML-CTF, becomes a general resource.[20]

4.26 Similarly, Liberty Victoria commented on the potential for reporting entities to make ancillary use of information they are required to collect:

> Some commentators have pointed to the commercial opportunities that this larger base of information provides with one calling it 'the greatest business lever' and another suggesting that 'financial institutions can turn their anti-

16 *Submission 40a,* pp 3–4.

17 *Submission 40,* p.4. Also, see *Submission 9*, pp 7–8.

18 *Submission 14,* p.3. Also, see *Submission 40,* p.4.

19 *Submission 9*, pp 7–8. Also, see, *Submission 40a,* p.2.

20 *Submission 9*, pp 7–8.

> money laundering compliance systems into robust surveillance and identification systems that deliver benefits well beyond the regulatory requirements'.[21]

Retention period for records

4.27 The APF expressed concerns on the requirement that records be retained for seven years.

> The Bill will require reporting entities to retain detailed records, including of customer identification, for seven years. This is a completely disproportionate requirement both in terms of the level of continuing intrusion and in terms of the compliance burden. It also creates a dangerous precedent for similar future requirements in other sectors and for other purposes. A proper application of privacy principles would see records kept for no longer than is necessary for the primary business purpose.[22]

Privacy Impact Assessment

4.28 A Privacy Impact Assessment (PIA) measures the privacy impacts posed by legislative, policy or technological initiatives. A PIA report should describe and de-mystify the initiative, identify and analyse the privacy implications, and make recommendations for minimising privacy intrusion, and maximising privacy protection – while ensuring that the initiative's objectives are met.[23]

4.29 The Department engaged the services of Salinger & Co to conduct a PIA on the Bill which concluded on 15 September 2006.

Key findings and recommendations

4.30 The key findings of the report included:

- widespread support for the objectives of tackling money-laundering and terrorism financing;
- concerns about whether the scheme will actually be effective in achieving those objectives;
- concerns that in some respects the proposal is disproportionate to the risks and overly intrusive into people's personal affairs;
- significant concerns about the collection, use and disclosure of personal information for purposes unrelated to the objectives of tackling money-laundering and terrorism financing; and

---

21 *Submission 1*, p.12.

22 *Submission 9*, p.6.

23 Salinger & Co, *Privacy impacts of the Anti-Money Laundering and Counter-Terrorism Financing Bill and Rules, 2006: A Privacy Impact Assessment for the Australian Government Attorney-General's Department* (2006), pp 5–6.

- an inadequate privacy control environment at several points in the scheme.[24]

4.31 The PIA report made 96 recommendations in total, of which some were identified as critical recommendations[25] and are briefly detailed below.

Scheme should be proportionate to risk

4.32 Industry, public interest representatives and people want and expect a system designed and targeted to find those committing money laundering or crimes at the 'serious end' of the scale, but not such that small or minor transactions (or even transgressions) are caught in the net as well.

Use of personal information should be limited to stated objectives

4.33 The PIA stated that disclosures to law enforcement authorities such as the AFP, ASIO, ATO and State and Territory police forces did not receive wide criticism from either industry or public interest representatives. Such disclosures are seen as being appropriate for the purpose of 'serious crime' such as money laundering, terrorism financing and tax evasion. However, the fact that AUSTRAC held data can be used by a range of agencies for varying purposes has raised a number of issues.

4.34 The PIA report made recommendations to limit the use of personal information collected under the scheme to purposes related to the investigation of money laundering, terrorism-financing, tax evasion or serious crime.

Extend the National Privacy Principles to all reporting entities

4.35 The PIA recommends the extension of the National Privacy Principles (NPP) to all reporting entities, but that where the NPPs are seen to be inadequate, more specific provisions should also be added to the Bill and Rules. Recommendations have also been made to ensure all recipient agencies are likewise covered by the Information Privacy Principles in the federal Privacy Act, if they are not already regulated by an equivalent scheme in their own jurisdiction.

Further work required

4.36 The PIA suggested that further work should be undertaken including:

- adequate time prior to commencement;
- the provision of guidance and education for reporting entities;
- an independent evaluation of operations to occur after two years; and
- the tranche 2 reforms not to proceed without considerable further thought, review and consultation.

---

24 Salinger & Co, p.99.

25 Salinger & Co, pp 100–104.

The Department's response to the Privacy Impact Assessment

4.37 The Department provided a formal response to the PIA and has adopted 30 recommendations with one recommendation still under consideration. The following responses[26] to the PIA were provided by the Department:

- While the impact on privacy should be minimised, the current global environment necessitates the need for a comprehensive and robust AML/CTF regime. The risk based approach is flexible and recognises the unique roll of business in preventing money laundering and terrorism financing. Risk based approaches have either been or are being adopted by FATF members.
- The Privacy Act will be amended to ensure that all reporting entities (including small businesses that are currently exempt) are subject to the NPPs in relation to their compliance with the AML/CTF regime.
- The Rules will be legislative instruments and as disallowable instruments will be subject to Parliamentary scrutiny. In addition, in performing its functions under the Bill, AUSTRAC is required to consult with the Office of the Federal Privacy Commissioner (subclause 212(2)).
- Designated government agencies under the proposed legislative package have a role to play in combating money laundering and terrorism financing and as such will have access to AUSTRAC information. Most of these agencies are already empowered for the same purposes under the *Financial Transaction Reports Act 1988* (FTRA). The addition of Commonwealth and State and Territory anti-corruption agencies is also important to detect corruption.
- There are jurisdictional limitations to extending privacy obligations to other non-Commonwealth agencies and foreign entities. While a complaint mechanism is desirable, it is unlikely that all relevant agencies from each State and Territory would consent to the jurisdiction of the Federal Privacy Commissioner.[27]

4.38 The Department specifically commented during the public hearing on the PIA recommendations relating to designated agencies having access to AUSTRAC held information and stated:

> Finally, 16 of the unaccepted recommendations related to the disclosure of personal information and protections against its misuse. We have some concern that these recommendations were based on a misconception of the purpose and use of AUSTRAC information, which in the end is of intelligence value only. That information does not of itself support a prosecution and can at best only lead to further investigation by authorised

26 Attorney-General's Department, Criminal Justice Division, *Privacy Impact Statement: Anti-Money Laundering and Counter-Terrorism Financing Bill & Rules* (2006) pp 3–4.

27 For further Department comment in response to the PIA, see *Committee Hansard*, 23 November 2006, p.33.

agencies in accordance with the rules which govern the conduct of those agencies.[28]

Criticism's of the Department's response to the PIA

4.39 Some witnesses expressed criticism that the PIA report was not made publicly available to stakeholders immediately upon completion, restricting the time available for consideration and comment by stakeholders.[29] The committee also heard from witnesses who were concerned that two-thirds of the PIA's recommendations were not accepted and who considered that the reasons provided by the Department for not adopting these recommendations were inadequate.[30]

28 *Committee Hansard*, 23 November 2006, p.33.

29 *Submission 1a*, p.3. Also, see, *Submission 9*, p.1.

30 *Submission 9*, p.1.