ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING BILL 2006

Submission by Australian Privacy Foundation

Key information missing or available at the eleventh hour, and then ignored

1. Much of the detail of the new regime will be contained in *AML-CTF Rules*, to be issued by AUSTRAC under the legislation. While draft *Rules* have been available, these have been made difficult to find from both AUSTRAC and AGD websites, frustrating attempts to fully understand the proposed scheme – specific enquiries were necessary to locate the Rules. It is essential that the draft rules be available during the Parliamentary debate on this Bill.

2. The Explanatory Memorandum includes *Financial Impact* and *Regulatory Impact statements*, and *Cost-Benefit Impact assessment* of various options, but no *Privacy Impact Assessment* as recommended by the Privacy Commissioner and endorsed as recently as August this year by the Attorney-General.

3. A Privacy Impact Assessment for the Bill and Rules, and the government's response, has now been made available to witnesses at the Committee's hearings in Melbourne on 14 November. The availability of these crucially important materials has not been made known to interested parties and even for those of us that have incidentally 'discovered' these documents, there is no realistic opportunity to review them and take them into account in our submissions. From a cursory initial reading of the PIA, it appears to support many of our concerns, as expressed below.

4. We note from the government's response to the PIA that the government has rejected at least 66 of the 96 recommendations of the independent Privacy Impact Assessment (in effect many more than that as some recommendations are only accepted to the extent that the Privacy Act provides protection, when in fact it does not[1]). Many of the recommendations are simply dismissed out of hand without reasons, while the justification for rejecting most of the others is not convincing.

5. The government's late release of the PIA, and its response, demonstrate a complete contempt for the PIA process. The Attorney-General's endorsement of PIAs is exposed as fraudulent window-dressing – the government clearly does not intend to take into

[1] The weakness of the Privacy Act also limits the value of the superficially positive removal of the small business organisation exemption from any reporting entities in relation to personal information handled under the AML-CTF legislation – item 152 of the AML-CTF (Transitional Provisions etc) Bill 2006 . The APF nonetheless welcomes this change to the extent that it does apply the National Privacy Principles to small reporting entities.

account or sensibly respond to PIA findings, and is not seriously interested in the contribution an independent PIA can make to the legislative process.

6. We urge the Committee to recommend deferral of the Bill to give an adequate opportunity for consideration of the Privacy Impact Assessment.

Neglect of privacy concerns throughout the development of the legislation

7. During more than two years of consultation, the government has failed to significantly address the major privacy concerns drawn to its attention by the APF, the Privacy Commissioner and other interested parties (and now it appears by the PIA). Throughout the consultation the government has favoured business interests, with special closed briefings and liaison. While AUSTRAC itself has made efforts to at least inform consumer groups through its privacy Consultative Committee, the government itself has consistently failed to even attempt to answer criticisms of the regime – it has simply continued to assert the need for a highly intrusive regime 'to comply with obligations under the Financial Action Task Force recommendations'.

8. Amongst the questions the government refuses to answer are:

- What is the international law basis for the FATF recommendations?
    - Far from being binding as claimed, they carry less formal weight than the government's obligations to protect privacy under the International Covenant on Civil and Political Rights. This appears to have been implicitly conceded in the notes to the Objects clause (cl.3)
- Which elements of the regime actually go well beyond the FATF Recommendations?
    - Many of our partners in FATF appear to be able to comply with much less intrusive reporting schemes, with narrower scope, higher thresholds, and more objective criteria
- Why is the government continuing to hide a broad based financial surveillance scheme, with multiple uses, behind the misleading label of Anti Money Laundering and Counter-Terrorist Financing?
    - Perhaps because it knows that directly giving these monitoring powers to the Tax Office, Centrelink or the Child Support Agency would be unacceptable?
- How can the general use of AUSTRAC data by such a wide range of agencies be justified on the basis of Objects (cl.3) which does not even mention purposes other than AML and CTF?
    - Again, could it be that the government dare not admit that the regime is used as a general resource for virtually all law enforcement, revenue protection and, increasingly, welfare compliance purposes?
- What will be the actual cost and compliance burden, particularly on the thousands of small businesses which will become 'reporting entities', required to conduct

onerous identity checks on customers, establish complex risk assessment and monitoring processes, and keep detailed records for seven years?

- The Financial Impact Statement, which is supposed to answer this question, puts it in the 'too-hard' basket, which if argued in relation to proposed privacy or consumer protection regulation would see it rejected out of hand.

Attempt to defer consideration of full impact

9. We note that it is still intended to defer designation of many non-financial businesses and professions until a second tranche of legislation. While this deferral will be welcome to the many thousands or real estate agents, jewellers and others who will eventually be covered, it is essential that the government is required to justify the entire proposed scope of the regime in the context of this first Bill. Otherwise, Parliament is being asked to approve an infrastructure and processes with only part of their 'downside' in focus.

Scope still massive

10. The Act will initially apply to 54 different financial services, 2 bullion services, 14 gambling services and an unspecified number of other services to be specified in Regulations (cl.6 Tables 1-4). It remains unclear as to whether and if so when, financial advisory services will be subject to the Act, and whether simply enquiring about opening an account will trigger identification and reporting requirements[2]. If they are, then there are major implications for individuals' ability to shop around for advice without being firstly 'pestered' by unwanted marketing, and secondly potentially 'dobbed in' as 'suspicious' – see below. The provision for a criminal offences for '[providing or receiving] a designated service using a false customer name or customer anonymity' (cl.139-140) not only hangs like a sword over anyone seeking to offer individuals simple advice, but also directly undermines the intent of National Privacy Principle 8 (anonymity).

11. The government is emphasising how it has responded to input (from business, not consumers!) by making the legislation more 'risk-based', to minimise the compliance burden. While this is fine rhetoric, the reality is that the legislation will still require most providers of designated services to establish detailed and potentially onerous customer identification procedures. This has major implications for the level of privacy intrusion in Australia, and cannot be divorced from a range of other 'identity management' initiatives. These include the *Document Verification Service* being established by the Attorney-General's Department, the Department of Human Services 'so-called' *Access Card* – in effect a national identity scheme, recent changes to the Electoral Act to allow access to the electoral roll for FTRA purposes (see separate discussion below), and the as yet uncertain effect of the Telecommunications (Integrated Number Database) Bill 2006 on access to telephone directory information (see our separate submission to Senators).

[2] The July revised Exposure Draft Bill suggested the application to financial advisory services had simply been deferred to the second tranche (AGD, Summary of changes)

False premise – single identities

12. All of these identity management initiatives start from a false premise – that individuals have a single 'identity' which can and should be readily compared and verified. The messy reality of humanity is that many people are legitimately known by different 'labels' in different contexts. They should not be forced to conform to some 'neat' bureaucratic numbering and labelling scheme. There may well be a particular problem in this respect for people from non Anglo-Celtic background, and significant potential for unfair discrimination based on unfamiliar name forms and combinations. The requirement for mandatory disclosure of other commonly used names (cl.141) compounds rather than relieves this problem. Many individuals may have simply lost track of the variations of name and initial combinations they have used in different contexts and could easily inadvertently commit this offence.

13. A wider and fuller debate about the relationship between these and other identity management initiatives (including many at State level and in relation to specific roles) is required.

14. Specifically suspicion '… on reasonable grounds that the person is not the person they claim to be' requires mandatory reporting under the fundamentally flawed 'suspicious matters' provisions (cl.41(d)&(e) (see below for more general criticism of these provisions). Given the likely number of 'mismatches' which will arise from the customer identity verification requirements, there is potential for very large numbers of innocent individuals to be listed on AUSTRACs secret blacklist, without their knowledge and with no recourse. There is also considerable potential for reporting entities and their employees, and customers themselves, to inadvertently fall foul of the offences of '[providing/receiving] a designated service using a false customer name ..' (cl.139-140).

Exclusion of stored value cards uncertain

15. While we welcome the setting of a monetary thresholds for stored value cards (cl.6 Table 1 Items 21-24), we are concerned that these thresholds can be changed, including reduced, by Regulation. There should be an absolute guarantee that holders of low-value stored value cards, such as telephone cards and public transport smart cards, will not be required to identify themselves – this would completely undermine the effect of National Privacy Principle 8 and similar provisions in State and Territory laws which defend individuals' right to anonymity.

16. As stored-value cards gradually replace cash, the anonymity of low-value cash transactions could become a thing of the past – no doubt a welcome prospect for the taxation authorities, but hardly the proper function of a law supposedly focused on serious crime.

Application to pre-paid mobile phone accounts

17. We understand that the definition of 'designated service' may cover pre-paid mobile phone accounts. If so, the customer identification requirements will effectively pre-empt the review of identification being undertaken by the Australian Communications and Media Authority. Several submissions in response to the ACMA Discussion Paper,

including ours, argued for the preservation of the option of anonymous pre-paid mobile accounts. There has been no progress report from ACMA, and it now appears that its review may be rendered redundant by the provisions of this Bill. No change to the identification requirements for pre-paid mobile accounts should be made without a full debate incorporating the submissions to and findings of the ACMA review.

Lack of reporting threshold disproportionate

18. The Bill continues the current FTRA requirement to report all International Funds Transfer Instructions (IFTIs), however small. The current lack of a threshold means that even the smallest wire transfers are included in the more than 11 million IFTI reports lodged in 2005-06[3]. While the Bill provides for a minimum value threshold to be set by Regulation, the EM expressly states that there is no current intention to invoke it. The absence of any threshold for IFTIs is a fundamental breach of the 'proportionality' principle underlying all privacy laws and instruments, and which we understood was also be a foundation principle of regulation under this government.

Suspicious matter reporting inherently flawed

19. The AUSTRAC Annual report shows an increase in the number of suspect transaction reports under the Financial Transaction Reports Act (FTRA) increasing by 44% in the last year to more than 24,000[4]. While no cumulative figure is given in the Report, it would be reasonable to assume that the total number of suspect transaction reports held by AUSTRAC, since it commenced operations in 1989, must now be in the hundreds of thousands.

20. These reports are based entirely on subjective criteria applied by employees of financial institutions, they remain on an AUSTRAC database indefinitely with access by (currently at least 29) partner agencies, and the individuals who are subject to the reports are never allowed to know that a report exists, due to a prohibition on notification and exemption from the FOI Act.

21. This Bill continues and expands the suspect reporting regime. The concept of 'suspicious transaction' is replaced by a new concept of 'suspicious matter' - much wider and even more subjective. It includes reasonable grounds to believe that a service or even prospective service may be relevant to the investigation of, or prosecution of a person for, an offence against [any] law of the Commonwealth or of a State or Territory. Any pretence that the law is focused on AML-CTF, or even serious and organised crime (as the FTRA was supposedly) appears to have been abandoned (see below under Access by agencies).

[3] AUSTRAC Annual Report 2005-06
[4] AUSTRAC Annual Report 2005-06

22. The new definition and criteria, together with the increased range of reporting entities and designated services subject to the reporting obligations, a significant increase in the number of reports can be expected.

23. In relation to money-laundering and terrorism financing, grounds for reporting include suspicion that 'provision, or prospective provision, of [a] service is preparatory to the commission of an offence' (cl.41(1) (g) & (i)). This 'speculative' element makes the judgment of the thousands of reporting entities even more subjective and unacceptable in relation to these already inherently subjective types of offences.

24. The prohibition on 'tipping off' is retained (cl.123) and suspicious transaction reports will remain off limits to individuals attempting to gain access or make corrections under either the Freedom of Information Act[5] or the Privacy Act.

25. At least under the existing FTRA, most cash dealers are large or medium sized organisations with professional staff who can be trained to exercise some judgement before making suspect transaction reports. 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?

26. Small businesses' relationships with their customers will be severely threatened by the knowledge that a wide range of factors may lead to a suspicious matter report. If asked by a customer "Are you telling any government agencies about me?" shop assistants and counter staff will in some cases be required by the Act to lie.

27. The massive extension of mandatory 'dobbing in', on the most subjective of grounds, by relatively inexperienced and unqualified private sector employees will be highly objectionable to most Australians. Spying on citizens on behalf of the State is not something we should find an acceptable role for Australian businesses.

Record keeping requirements disproportionate

28. 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. Interests of law enforcement and revenue protection and other government bodies should be accommodated by arrangements for access, with appropriate authority and justification, during the period they are required by the business, together with an

[5] Confirmed by item 148 of the AML and CTF (Transitional Provisions etc) Bill 2006

exceptional provision for *preservation* of records on request in relation to particular investigations.

29. Allowing 'speculative' government needs for access to data to determine retention periods is contrary to a sound application of privacy principles, and should be resisted.

Sharing of information within business groups dangerous

30. The exemption from the non-disclosure provisions for information sharing within 'designated business groups' (cl.123(7)) appears to create an undesirable potential for effective 'blacklisting' of customers based on the subjective assessments by just one of a group of businesses, which do not appear to even need to be related in an ownership or control sense. Much greater detail is needed on what sorts of information could be shared, between whom, and what controls and safeguards would apply to its use by businesses forming part of a group.

31. In particular, it is unclear as to whether this exemption could be used to justify the sharing of customer identification and risk assessment information, irrespective of any 'reports', in a way which would undermine the effect of the Privacy Act in limiting marketing uses of information without consent. The Privacy Commissioner should be asked specifically to comment on this possibility.

AML-CTF Risk Assessments – cautious welcome for concession

32. This appears to be one area in which the government may have heeded some of the privacy concerns, although it was no doubt also an area of significant compliance burden concern to business. The draft Bill's requirement for all reporting entities to implement an AML-CTF Program, with risk assessment of potentially all customers, has been replaced with a discretionary power for the AUSTRAC CEO to require specific reporting entities to undertake and report on risk assessment (cl.165). Whether this amounts to a significant concession will depend on how the power is used.

33. The EM expressly 're-assures' reporting entities that their AML-CTF Programs will not need to be made public. This is of little comfort to the individuals whose privacy will be affected – there would be appear to be no accountability to ensure that reporting entities do not go 'over the top' in their risk assessment and monitoring activities, 'to be on the safe side' – particularly in light of the criminal penalties. The whole scheme is weighted in favour of 'over-compliance', with insufficient safeguards for individuals.

Access to AUSTRAC information by agencies still out of control

34. The Bill confirms that the ATO and at least 30 other 'Designated Agencies'[6] can in effect use AUSTRAC information for *any* of their functions[7]. There is no attempt to limit

[6] Designated agencies is defined in the Bill as including more than 30 specific Commonwealth, State and Territory agencies

[7] Of all the 'Designated agencies' only the Treasury is limited in the uses it can make of AUSTRAC information (cl.126(5)&(6)).

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 – directly for at least the 30 Commonwealth, State and Territory agencies, and indirectly to a potentially unlimited range of other government agencies both Australian and foreign in the context of investigations (subject only to a limitation on disclosure of suspicious matter reports which are 'only' (sic) available to the 30+ designated agencies).

35. The intended safeguard of requiring non-Commonwealth recipients to agree to comply with the IPPs in the Privacy Act (cl.126(3)) is, as the Privacy Commissioner has pointed out, of limited value given the lack of enforceable remedies for any breaches, and her jurisdictional inability to investigate those agencies. The supposed safeguards in relation to foreign governments – obtaining 'appropriate undertakings'[8]- are even less credible, and directly undermine the emerging controls on transborder data flows considered suitable for the private sector (NPP9) and for the Victorian and NT public sectors[9], but apparently not for the Commonwealth itself.[10]

Abuse of Electoral Act

36. Items 13-17 of the AML and CTF (Transitional Provisions etc) Bill 2006 confirm the availability of electoral roll information to reporting entities for the purposes of customer verification under the AML-CTF legislation. While these provisions simply replicate the recent changes that allowed access for FTRA verification, we repeat the concerns expressed in our submission to the Senate Finance and Public Administration Committee Inquiry on the Electoral and Referendum Amendment (Electoral Integrity and Other Measures) Bill 2005. In particular, we note that the amendments to the electoral law still pretend to limit the purpose for which reporting entities can use electoral roll information (item 16). As we explained to the F&PA Committee:

> "We submit that this is an impracticable and ineffective attempt. It will be impossible for 'cash dealers' [now reporting entities] accessing electoral information for identity verification not to make use of it for their own business purposes. 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.
>
> Allowing access to the electoral roll for FTRA [now AML-CTF] identity verification effectively amounts to allowing its use for updating customer records.
> …
> As well as this being a concern in itself, the competitive advantage that access to official name/address information will give to FTRA [now AML-CTF} reporting

[8] Clauses 132(1)(3) & (6) & 133(1)
[9] *Information Privacy Act 2000 (Vic)*, Schedule 1 IPP 9, and *Information Act (NT)*, Schedule, IPP 9.
[10] This remains a matter of contention in relation to the European Union's assessment of the adequacy of Australia's privacy laws, and related provisions in the privacy laws of some other jurisdictions.

entities will inevitably lead to pressure from other businesses for access, on competitive neutrality grounds. It seems likely that any pretence of restricting 'commercial use' [of electoral roll information] will soon be found to be impracticable and be abandoned."

Contact for this submission:

Nigel Waters, Board Member and Policy Coordinator
Australian Privacy Foundation
E-mail: enquiries@privacy.org.au
APF Web site: http://www.privacy.org.au