Anti-Money Laundering/Counter-Terrorism Financing Legislation

Consultation on Revised Exposure Draft Bill and Rules

(at www.ag.gov.au/aml)

Australian Privacy Foundation submission to Attorney-General's Department and AUSTRAC, August 2006

CONTENTS

The Australian Privacy Foundation

1. The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. Relying entirely on volunteer effort, the Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions. The Foundation uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For information about the Foundation and the Charter, see www.privacy.org.au

Revised scheme

2. While we welcome the opportunity to comment on the revised proposals, the extremely short consultation period has made it difficult for us to review the changes in detail, and is an unsatisfactory basis for proceeding with these significant changes.

3. We gain the impression that most of the changes are a response to industry concerns about the compliance burden rather than to concerns expressed by ourselves and other public interest groups about the disproportionate nature of the legislative regime. The changes have not even responded to some of the key criticisms made by the Senate Legal & Constitutional Committee in its April 2006 report on the Exposure Draft of the Bill.

4. Most of the criticisms made in our April 2006 submission remain valid in respect of the revised Bill and Rules. We comment on both in the one submission as many of our concerns relate to their interaction.

5. While the greater emphasis on a risk-based approach is welcome in some respects, it has the perverse effect of increasing element of subjective judgement by unqualified employees of businesses who are unqualified to make such judgments, many of which could be highly prejudicial to individuals – resulting effectively in secret blacklisting and discrimination.

6. The scheme remains, in our view, fundamentally flawed, involving a highly privacy intrusive regime of routine surveillance with uses far beyond the declared objectives, and justification, of fighting serious and organised crime, including terrorism.

7. We set out below some of main remaining concerns, with particular emphasis on the changes in the revised Bill and Rules. We do not however repeat all of the concerns in our April submission, others of which have not been addressed and which remain applicable to the revised scheme.

Inadequate justification for the Bill

8. The justification for the Bill, by reference to 'international obligations' in the areas of money-laundering and terrorist financing remains weak and poorly explained – we suggest because it would not stand up to serious scrutiny. It is clear from international comparisons that there is considerable flexibility for signatories to interpret the FATF Recommendations (which are just that and not binding treaty obligations), and not all other jurisdictions are putting in place such a comprehensive identification, reporting and monitoring regime.

Seriously misleading title and objects

9. There remains a serious 'truth in legislation' issue – as we said in our April submission, it is simply dishonest to present this legislation as being solely about countering money laundering and terrorist financing. Both the Title and the Objects clause (S.3) convey this misleading impression. The true wider purpose of the legislation is only revealed in later clauses, including ss.39(1)(f)(iii)-(vii); ss.98(1)); and ss.99(1)).

10. There appears to be no statutory limitation on what agencies/functions AUSTRAC could designate as users of AUSTRAC data – and the Bill expressly envisages the inclusion of State/Territory agencies (Ss.99(3)) and foreign countries (S.103).

11. The use of AUSTRAC information under the existing Financial Transaction Reports Act 1988 (FTR Act) has already spread well beyond the original focus of serious and organised crime (used to justify the FTR Act's major incursions into financial privacy) – most recently by giving access to Centrelink and the Child Support Agency[1]. The new Bill appears to provide the basis for an *unlimited* range of uses for AUSTRAC information, without this being acknowledged in the Objects clause or reflected in the Short title.

12. As we said in April, this draft Bill would more accurately be titled 'a Bill to routinely monitor the financial affairs of all Australians', or the 'Invasion of Financial Privacy Bill'.

13. In effect, AUSTRAC information will be, even more than at present, a general resource available potentially to any agency of any government for any purpose.

14. The Senate Committee recognised these concerns and recommended a clearer objective statement (at paragraphs 4.76 & 4.77 of its Report) but this appears to have been ignored.

First and second tranches

15. The government had already cleverly, but cynically, deferred the planned application of the regime to major new areas of business (real estate, lawyers and accountants acting in a non-financial capacity, jewellers) until a second round of legislation to follow in a few years. The summary of the revised Bill explains that even more of the new areas – specifically the application to financial advisers - have been deferred until the second tranche – temporarily deferring this controversial and problematic area which would bring the intrusiveness of the scheme into clearer focus for more indivisuals.

16. The revised Bill still lays the foundations and builds the infrastructure for further expansion, which needs to be part of the current debate. If this Bill continues to implement only the first tranche, then there must at least be an acknowledgement by and explanation by government, when the Bill is introduced, that sets out the full intentions and impact of the first and second tranches together.

History of progressive function creep

17. APF believes that if more people knew about the existing FTR Act regime, there would already be significant public disquiet. The regime offends against several fundamental privacy principles, and may never have been accepted in its present form had it not been enacted (originally as the Cash Transaction Reports Act) just *before* the Privacy Act itself in 1988. It also makes a mockery of continued assurances about banking confidentiality.

[1] 2004 amendment to the Financial Transaction Reports Act.

18. The CTR/FTR Act has been significantly amended since 1988, increasing the range of agencies with access to AUSTRAC data, and the purposes for which they can use the data, and authorising more direct on-line access (thereby weakening control and accountability).

Major objections

19. The major objections to the legislation – both to the existing FTRA and with even more force to the proposed new law even as revised – remain as follows:

- A complete lack of **proportionality** – the only statutory thresholds are $10,000 for significant transactions (which does not apply to suspect and international transactions, and which in any case is gradually being eliminated by inflation), and a proposed $1000 threshold for stored value cards. There are no other thresholds – *all* new customers have to be identified and *all* transactions monitored and/or reported. There has been only a limited attempt to identify risk factors or measure the scale of alleged abuses in such a way as to relieve many Australians, and many transactions, from the scope of the scheme. The new Bill includes provision for some relief from re-verification of identity in relation to existing customers, but this will make only a minor difference in the longer term.

- Unacceptable **secrecy** – suspect transaction reports are expressly exempt from access under the FOI and Privacy Acts, and it is an offence to notify a customer that a suspect transaction report has been lodged. The suspect transaction database amounts to a secret blacklist, based on extremely subjective criteria and unverified judgements, which could seriously prejudice individuals listed on it without their knowledge and without any possibility of challenge, or remedies. While not clear, it appears that the same secrecy may apply to a subjective 'risk classification' made of *all* new customers. This secrecy not only denies individuals their normal **access and correction** rights, but also arguably also offends against the **data quality** principle, in that there is only limited quality control on the accuracy of suspect transaction reports, and risk classifications.

- Progressive expansion or **function creep**, well beyond the areas of serious and organised crime originally used to justify the extraordinary privacy intrusions. This has already taken the scheme into routine use for a wide range of less serious offences, including minor welfare and tax transgressions, and will accelerate under the new legislation.

- The function creep has also involved a major expansion in the number of agencies accessing AUSTRAC data, most of them direct online connections, which not only offends against **purpose limitation** principles, but also risks **security**, in that the chances of unauthorised access and use, despite AUSTRAC's best endeavours in security measures, are continually increasing.

Detailed comment on the Revised Bill and Rules

Introduction (Part 1)

Designated services

20. We still have no estimate of the numbers of reporting entities expected to fall into one or more of these categories in the Table in section 6 and therefore incur obligations under the law. We again urge the government to include such estimates in its Regulatory Impact Statement so that Parliament, and the community, can make an informed assessment of the proportionality of the legislation.

21. Our argument about the illogical approach to value thresholds (at paragraphs 25-27 of our April submission) appears to have been ignored, with no attempt made to justify the inconsistent approach.

22. We remain very concerned about the scale of the additional intrusion into individuals financial affairs that will result from the legislation, and suggest that many of the requirements – for various 'programs' – to be placed on a large number of smaller businesses are completely disproportionate – certainly to the unquantified risks of money-laundering and terrorist financing, and even to the wider set of objectives discussed above.

Designated business group

23. We note the introduction of a new concept of 'designated business group', and consequential changes to Part 7 (joint programs – clause 74(3) & Part 11 (disclosure to related entities clause 95(7)). While we can see some advantages in this in allowing centralised, and therefore potentially more professional handling of compliance matters, there are also potential risks. In particular it could compound the problem of blacklisting and discrimination by widening the range of organisations who become aware of potentially ill-founded, yet highly prejudicial reports about individuals. We continue to draw attention to the lack of any 'natural justice' provisions that would allow individuals to even be aware of, let alone challenge, 'suspect transaction' reports – see further below under Reporting requirements.

Identification requirements (Part 2)

24. The full implications of the identification requirements (Part 2) can only be assessed in light of the draft Identification Rules – now Chapters 2-6 of the revised Rules.

25. We welcome the inclusion in Part 2, Division 3 of an additional risk-based criterion for low-risk services, to which modified (lesser) identification requirements will apply. The link to 'suspicious matters' should mean that there is no need to re-verify the identity of the majority of existing customers. But we read the provisions as still requiring initial customer identification from all *new* customers. If this is correct, then the concession is very limited – and can hardly be portrayed as a significant shift to a risk-based approach.

26. We submit that the new emphasis on risk based identification requirements should be carried through into the complete removal of identification requirements for low risk services.

Verification of customer identification information

27. The revised Rules now contain further details of the verification requirements. They include a safe-harbour scheme of reduced requirements for 'lower-risk' customers. While we give 'in-principle' support to more proportional risk-based requirements, it appears that in some respects they have been made more onerous and intrusive. The requirements for individual customers are set out in Chapter 2.2 and 2.9.1-2.9.3. but it is not clear how these requirements will compare to the current '100 point check' requirements.

28. We note that the Rules now make express reference to credit history at 2.2.14(b)(iii). We have not had the time to investigate the relationship of this to the permitted uses of credit information under the Privacy Act but the government must explain how they relate.

29. Once again, we stress that in order to fully assess the privacy implications of the verification of identity requirements, it is necessary to comprehend how the obligations of reporting entities will interact with a number of other government initiatives. These include:

- The Document Verification Service, currently being piloted
- Recent amendments to the Electoral Act to allow organisations with obligations under the existing FTR Act to access electoral roll information for verification purposes
- Pending amendments to the Electoral Act to require enhanced evidence of identity for electoral enrolment
- The Department of Human Services so-called 'Access Card' and the associated universal registration, effectively mandatory, of the entire Australian population.
- Various other identity management initiatives

30. Unless any one of these initiatives is considered in the wider identity management context, there is a risk that the aggregate loss of privacy will be greater than is apparent from any one initiative.

31. The government should explain how these various initiatives interact, and allow a reasonable period for debate of the relationships and overall impact on privacy, before proceeding with any one of them.

Reporting requirements (Part 3)

Suspicious matters reports

32. The reporting requirements for 'suspicious matters' – even more subjective than the current 'suspicious transactions' - remain fundamentally flawed.

33. We submit that the whole concept of reporting 'suspicions' by employees of reporting entities who are not qualified and trained investigators is inherently flawed, and needs to be re-thought.

34.The revised Bill now includes as specific 'grounds for suspicion' a suspicion that the customer (or agent) is not the person they claim to be' (clause 39(1)(d) & (e) (and draft Rule 2.2.10). This is fraught with danger. There must be a wide range of circumstances, and large number of instances, where individuals have to discuss questions of identity with businesses – examples include married women using their birth name, and individuals attempting to bank cheques that have been made out to them in 'known as' names. It would be ludicrous to suggest that reporting entities should treat all such discussions as grounds for a suspicious matter report. To avoid such a result, these provisions either need to be withdrawn or at least significantly re-drafted (see also clause 110, about which we comment further below).

35. We note that the revised draft Rules no longer contain any other suggested grounds or criteria for 'suspicion'. We assume that it is now the intention to issue guidance later. This is unacceptable – it merely defers consideration of one of the most controversial and sensitive issues surrounding the reporting regime, which needs to be debated during the passage of the legislation.

36. The criteria suggested in AUSTRAC guidance on suspect transaction reporting under the FTRA have always been highly subjective. The requirements in original draft AML/CTF Rules on Suspicious Matter Reporting were no better. They included appearance and behavioural factors as well as supposedly factual matters which there is no reason for employees of reporting entities to know. The result of the broad and subjective guidance, and of the penalties for failure to report, will be either:

- Even greater intrusion into customers' personal affairs, often based on 'guesswork', and/or,
- Over-reporting because of an absence of information – 'to be on the safe side',

37. There remains a serious risk of over-reporting of indigenous people or people of a non-English speaking background, because of prejudice, discrimination or misunderstandings of different cultural norms of behaviour.

Inconsistent scope of reporting requirement

38. As a result of the new risk based approach, there appears to be a discrepancy between the assessment of risk – which is defined, properly, as only money-laundering and terrorism financing (ML/TF) risk in the identification; ongoing due diligence and AML-CTF Program Rules, but still involves a much wider set of offences in the suspicious matter reporting provisions – specifically clause 39(1)(f)-(h) of the Bill. This discrepancy serves to highlight the extent of the function creep that has already occurred in the existing legislation and is being confirmed in the new scheme, at least in respect of the reporting regime.

39. The 'suspicious matters' reporting requirement must be limited to much more objective criteria, linked clearly to the anti-money laundering and counter terrorism objectives and to the ML/TF risk on which the other parts of the Bill are now based.

Relationship to secrecy provisions

40. We re-iterate our contention that the 'suspicion' reporting regime cannot be divorced from the legislative prohibition on notifying the subject of the report (the 'tipping-off' offence in clause 95). The inclusion of an individual on AUSTRAC's suspect [transactions/matters] database, accessible to more than 30 agencies, has the potential to adversely affect them, even if they are not aware of the effect.

41. We accept that there would be occasions on which a suspicion was so strong that it led to immediate action by appropriate authorities, and in such cases, 'tipping off' would clearly be inappropriate. However, in the majority of cases where no action is considered necessary there is no good reason why the subject of the report should not be notified – at least after a short interval.

42. At least if the individuals concerned were notified, they would have the opportunity to challenge the reasons for the report. 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 and these provisions must be repealed, or replaced with a reporting regime that incorporates review rights based on natural justice principles.

Threshold transactions

43. We note that these have been defined (in clause 5) as not less than $10,000 (the current level under the FTRA) but with provision for variation by Regulation – but only a downwards variation. We contend that there needs to be provision for *increasing* the thresholds, particularly in light of the progressive effect of inflation. The threshold amounts should either be expressly defined to allow for indexation or provide for periodic increases.

International Funds Transfer Reports

44. We strongly urge the government set a monetary threshold for International Funds Transfer Instructions required to be reported - either by regulation under s.42 (1)(e), or preferably in the legislation itself.

Exemptions from reporting requirements

45. We welcome the addition of provisions allowing for exemptions from the various reporting requirements, (clauses 40A, 41A and 43A) but we consider that this should not be left to as yet unspecified Rules to be issued by AUSTRAC. The legislation itself should grant some exemptions and give guidance as to what the criteria for further exemptions by Regulation could be.

Monitoring requirements – AML/CTF Programs (Part 7)

46. The revised Rules for AML/CTF Programs (Chapter 8) are far less specific than the original draft Rules. While we welcome a risk based approach clearly focussed on ML/TF risk (as a more proportional response to the original objective), there may be adverse consequences in the implementation.

47. It is no longer clear if reporting entities will be required to classify every customer according to risk criteria (as was suggested in the original Draft Rule, AML/CTF Programs, paragraph 14).

48. If so, it remains unclear if reporting entities will be allowed to inform customers of their risk classification – we re-iterate our suggestion that they should be *required* to do so, as well as having to respond to enquiries under National Privacy Principle 6, and that there must be a mechanism for challenging assessments.

49. It is no longer clear if AML-CTF Programs will require the routine monitoring of *all* customers and *all* transactions, even those which are classified as low risk. The relationship of *minimum KYC information* is to *additional KYC information* and *enhanced due diligence* requirements is no longer spelt out. We assume that further guidance will need to be given in due course. However, because these requirements will significantly affect the level and breadth of privacy intrusion, they need to be detailed and debated during the passage of the legislation.

50. We re-iterate our concern about the *employee due diligence* programs required by the draft Rules (Chapter 8.3), and our call for reporting entities to lose the employee records exemption in the Privacy Act 1988 in respect of such programs. As previously stated, this would in practice be impossible to separate AML-CTF generated records from other personnel information and the obvious solution is a complete abolition of the employee record exemption, as already recommended by the Senate Legal & Constitutional References Committee[2].

[2] *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005, Recommendation 13.

Record-keeping requirements (Part 10)

51. We note that a record retention period of 7 years has now been set in the legislation (various clauses) The summary of the revised Bill does not explain or justify this length of time and we again refer to the tension with the objective of National Privacy Principle 4.2, particularly in relation to suspicious matters reports which will be hidden from the individual, and yet prejudicial, for a very long period – increasing the need for notification and review rights.

Secrecy and Access (Part 11)

Secrecy

52. We have already noted above our serious concern about the express secrecy of suspicious matter reports (s.95) . To the extent that direct access rights cannot apply, we submit that individuals should be able to apply to an 'intermediary' for re-assurance that any information held about them by AUSTRAC is held in accordance with privacy principles. There are precedents for 'intermediary' access and re-assurance both in the Privacy and FOI Acts (e.g. in relation to sensitive health information) and also in relation to the intelligence agencies, where the Inspector-General of Intelligence and Security performs such a role.

Disclosure

53. We re-iterate our concerns that the secrecy provisions (clauses 93-94) need to include appropriate exceptions both for Privacy/FOI subject access, and for disclosure to a range of public officials investigating complaints from individuals (including the Privacy Commissioner, HREOC, the Ombudsman and the IGIS), and to courts and tribunals in relation to challenges by individuals. The present drafting of Part 11 would appear to constrain AUSTRAC and reporting entities from cooperating with any investigations or court/tribunal proceedings brought by an aggrieved individual.

Access by agencies

54. The provisions in Part 11 Division 4, together with the definition of 'designated agency' still leave open a potentially unlimited range of uses of AUSTRAC information, including for purposes completely unrelated to money laundering or terrorism financing, or even to AUSTRAC's own functions.

55.The access provisions must be substantially redrafted to be much more tightly focussed on anti-money laundering and counter terrorism objectives, unless the Government is prepared to be open about, and justify, a broader scope.

56. The Bill seeks to impose conditions on disclosure designed to protect individuals' privacy (clauses 99(3), 103(3) and 104(1).

57. While some (but not all) of these provisions require undertakings to comply with the IPPs of the Privacy Act, we continue to question how effective the provisions can be given the unenforceability of any assurances given. We again suggest that a preferred approach would be to borrow elements of National Privacy Principle 9, by only allowing disclosure to third parties which are bound by equivalent and enforceable privacy principles (such as the Victorian Information Privacy Act and various overseas Privacy Laws that have been assessed by the European Commission as meeting the standard of adequacy under the European Union Data Protection Directive).

58. If any disclosures are allowed to agencies *not* subject to equivalent and enforceable principles, then the requirement to seek undertakings of compliance should be replaced by express provision for requiring contractual obligations to bind the recipient agencies to equivalent principles to those in the Privacy Act, with the Australian Privacy Commissioner tasked with the power to investigate complaints and audit their uses of AUSTRAC information, and for termination or limitation of any disclosure arrangements in the event of misuse.

Offences (Part 12)

59. We re-iterate our concerns about s.110, which imposes wholly unreasonable obligations on reporting entities in relation to 'false names', whatever that means (see discussion of new clause 39(1)(d) & (e) above), and in relation to anonymity, which directly overrides National Privacy Principle 8. While this override can be justified in relation to a much more focussed regime, we submit that it is inappropriate to override the effect of NPP8 for such a far-reaching and unlimited range of uses, where customer identification is required for all designated services, without significant exemptions for small matters.

60. The offence provisions remain unbalanced in that they focus on actions which undermine the objectives of the regime. They should be balanced by the creation of serious criminal offences for unauthorised use of information collected for, held by, or obtained from AUSTRAC.

Audits, Information-gathering and Enforcement (Part 13-15)

61. We have grave concerns about the proportionality of the powers granted by these Parts, and seek clarification of the relationship between the Information-gathering powers in Part 14 and the power to issue Notices (including to produce information) in Part 15. In principle, any power to require production of personal information should be subject to independent oversight – preferably through a court issued warrant system. There is a serious risk that agencies such as AUSTRAC are being given greater powers, with fewer safeguards, than police.

Coverage and Application of Privacy Act

Removal of small business exemption for all reporting entities

62. Many reporting entities under the new legislation would be exempt from the *Privacy Act 1988* under the small business exemption from that Act. Given that the personal information that will be collected will be as a direct result of government policy, it is essential that the information be afforded the same protection, and individuals given the same rights, as would apply if the information was collected directly by government agencies. We submit that any organisation with obligations under the so called AML/CTF legislation *must* automatically lose any exemption they may enjoy from the Privacy Act.

Enforcement of Privacy Act notice requirements

63. We restate our concern about enforcement of compliance by reporting entities with the requirements of NPP1.3 (or 1.5) to ensure that individuals about whom information is collected are made aware of certain matters. We urge the government to introduce

- Audit powers (and accompanying resources) for the Privacy Commissioner in relation to the NPPs
- A specific requirement in the AML/CTF legislation for reporting entities to notify customers about the reporting regime at the time of each reportable transaction – to reinforce and make more specific the NPP 1 requirement
- An obligation on AUSTRAC to issue guidance on, and proactively monitor, the requirement to give appropriate notice

Privacy Impact Assessment

63. We are aware that requests for tender were issued in late July for a Privacy Impact Assessment. We welcome this as consistent with recommendations from ourselves, the Privacy Commissioner and the Senate Committee. We caution however that the PIA will only be as good as the terms of reference allow and that its value will be limited unless it is made public – as the Privacy Commissioner's Guide to PIAs strongly recommends.

64. We look forward to the PIA being made public no later than the introduction of the legislation to Parliament, to assist parliamentary and community debate about the balance of public interests.

Australian Privacy Foundation
August 2006

E-mail: enquiries@privacy.org.au
Web site:http://www.privacy.org.au