Anti-Money Laundering/Counter-Terrorism Financing Legislation

Senate Legal & Constitutional Committee Inquiry into Exposure Draft Bill, Rules and Guidelines

(at http://www.aph.gov.au/senate/committee/legcon_ctte/anti-money_laundering/index.htm)

Australian Privacy Foundation submission, March 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

Lack of transparency during development of proposals

2. While we welcome the current opportunity for consultation, we draw attention to the lengthy period during which consumer representatives were effectively cut out of the process of developing the proposal and draft legislation.

3. A round of public consultation in early 2004 was spoilt by the failure of the interdepartmental working party to publish submissions. APF had to apply for them under Freedom of Information legislation, and were effectively denied timely access due to inordinate delays and the imposition of charges.

4. Between March 2004 and December 2005 – a period of more than 18 months – the government consulted in depth with industry bodies, but not with consumer, privacy or civil liberties groups. This has, not surprisingly, resulted in unbalanced draft legislation and rules which, to the extent that they have been improved by consultation do so only incidentally as a result of industry concerns about the compliance burden, rather than due to any acknowledgement of privacy and civil liberties concerns.

Seriously misleading title of the legislation, and omissions from Objects clause

5. There is a serious 'truth in legislation' issue here – 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, such as:

- the obligation to report suspicious transactions that may be relevant to "the investigation …. of an evasion ..of a taxation law; or …an offence against [any] law …." (Ss.39(1)(d)(i) and (ii);
- 'The Commissioner of Taxation … is entitled to access to AUSTRAC information for any purpose relating to …. a taxation law.' (Ss.98(1)); and
- 'AUSTRAC may .. authorise … specified officials of a specified designated agency to have access … for the purposes of performing the agency's functions …' (Ss.99(1))

6. There appears to be no statutory limitation on what agencies/functions AUSTRAC could designate – and the Bill expressly envisages the inclusion of State/Territory agencies (Ss.99(2)) and foreign countries (S.103).

7. 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.

8. 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'.

9. 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.

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

10. Like the FTR Act, the new legislation has four main elements:
- A customer identification requirement – innocuously described as 'due diligence' or 'know your customer'.
- Reporting requirements – in summary all transactions greater than $10,000; all international transfers (however small), and any suspect transactions (very subjective criteria for grounds for suspicion).
- AUSTRAC's role as the collator of all reports (already a massive database), and in analysing the data for patterns and financial intelligence.
- A dissemination regime whereby more than 30 Commonwealth, State and Territory agencies (mainly law enforcement and revenue protection, but increasingly others) are provided with on-line access to the AUSTRAC databases for an increasingly wide range of uses. Some of these agencies are also authorised to disclose AUSTRAC information to overseas authorities.

11. The proposed new law departs significantly from the existing FTR Act by:
- Significantly expanding the range of organisations subject to the law (63 different categories of business in the first tranche alone, with many more to follow in a second tranche),
- Tightening the already intrusive customer identification and monitoring requirements, and
- Increasing the subjective assessment element of the law from 'suspect' transactions to all customers. The extent of the information to be recorded about each customer, and in some cases reported, will depend on a risk classification for each new customer.

12. The government has 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. But the current Bill lays the foundations and builds the infrastructure for that 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 accompanying paper that sets out the full intentions and impact of the first and second tranches together.

13. 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.

14. 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

15. The major objections to the legislation – both to the existing law and with even more force to the proposed new law – are 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* customers have to be identified and *all* transactions monitored and/or reported. There has been no 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 identification and re-verification to be effected by AML/CTF Rules, but this relies too much on AUSTRAC – we think some exemptions should be included in the legislation itself.

- 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 analysis of Bill and Rules

16. We note that the first tranche legislation (the Exposure Bill) would only supercede those parts of the FTR Act applying to financial services. The FTR Act would remain in force, although significantly amended, until the second tranche of legislation applied to all non-financial services matters, at which point it would be repealed.

Justification for the Bill

17. The Objects clause (Section 3) focuses almost entirely on the need to meet 'international obligations' in the areas of money-laundering and terrorist financing – specifically the Financial Action Task Force (FATF) Recommendations. Apart from being seriously misleading by omission (see above), this focus is not supported by any rigorous analysis of what is actually required to meet those Recommendations.

18. In the course of recent consultation, the Australian Government Attorney General's Department have stated there is a secondary objective – not to wind back any of the requirements and effects of the existing FTR Act, *whether or not* they are strictly necessary to meet the FATF Recommendations.

19. It is clear from international comparisons that there is considerable flexibility for signatories to interpret the Recommendations, and not all other jurisdictions are putting in place such a comprehensive identification, reporting and monitoring regime.

20. We submit that the Australian Government is being highly selective in using the FATF Recommendations to support its wider policy objectives where it suits, and at the same time being deliberately vague about those aspects of the existing FTR Act, and draft Bill, which go beyond the FATF requirements.

21. It also appears that the FATF Recommendations are not 'binding treaty obligations', and do not therefore have to be slavishly followed by the Australian Government. The references in the Objects clause to international obligations seem primarily intended to provide a constitutional basis for the legislation.

22. The government should provide a clearer analysis of the need for all the elements of the regime by reference to specific international obligations.

23. We also note that the Australian Government has international obligations in relation to the protection of privacy, as signatory to the International Covenant on Civil and Political Rights (ICCPR) which should be no less significant than those cited in Section 3 of this Bill when seeking to strike a balance[2].

Scope and coverage – Designated services

24. The Bill introduces the concept of designated services to 'capture' reporting entities, with a table of 63 services in Section 6. There is no attempt to quantify the numbers of entities expected to fall into one or more of these categories and therefore incur obligations under the law. We submit that no sensible assessment can be made of the proportionality of the legislation without some estimates of the number of entities, and particularly small businesses and individuals, who will be subject to customer identification, reporting and monitoring obligations. We assume that estimates will have to be made for the purpose of a Regulatory Impact Statement in due course, but in our view estimates are required now so that the true impact of the legislation can be assessed.

25. We note that monetary thresholds are proposed in relation to some categories of designated service, specifically stored value cards (Items 21 and 22 in the table at Section 6). We welcome this recognition that it would be disproportionately burdensome to apply the law to cards limited to lower values, but cannot see why the same recognition has not been given to the wider range of designated services.

26. Apart from any other justification, surely an exemption for stored value cards effectively negates coverage of any other type of transaction of less than the stored value threshold? Anyone seeking opportunities for untraceable money laundering will simply be able to use stored value cards. Once the case for an exemption value threshold is made, it should be applied across the board. This should include the introduction of a threshold for International Funds Transfer Instruction reporting.

27. If the Government believes that small value transactions are being used for illicit purposes, it needs to provide some evidence, and also explain why a threshold for stored value cards is nonetheless proposed as acceptable. The current proposals are inconsistent in this respect, and suggest that thresholds could be introduced more generally without significantly detracting from the value of the regime for its primary objectives.

28. We are particularly concerned about the effect of the new approach in relation to financial advice. There are specific concerns about the effect on individuals' ability to search for an acceptable financial advisor without identifying themselves (and the relationship to the anonymity privacy principle) which we take up later. But there is also a wider question of the range of advisory services that will fall under the new law – there are many thousands of financial advisers and planners, as well as solicitors and accountants acting in a financial advisory capacity. These advisers – often sole practitioners – will acquire obligations under the law with customer identification, reporting and monitoring requirements which will be extremely onerous both for the service provider and for the customer or client.

29. In our view this is perhaps the most extreme example of the lack of proportionality in the Bill - although the proposed 'second tranche' extension to real estate industry will no doubt rival if not exceed it.

[2] see recitals in the Privacy Act 1988, and ICCPR Article 17.

30. Outside the privacy context, we would expect the burden and inevitable cost of compliance by small financial advisers and planners to have significant implications for the availability and affordability of financial advice at a time when governments are expecting individuals to take increasing responsibility for their financial security. We strongly urge the Government to consult consumer representatives operating in the financial area about the implications of this scope extension.

Identification requirements (Part 2)

31. These are described in the Bill as 'customer due diligence' requirements. We strongly believe that this is a business term which disguises the true effect and implications.

32. The full implications of the identification requirements can only be assessed once the relevant draft Rules are available. Only preliminary guidance on identification requirements has been made available as part of the package, and we reserve our final position on this aspect of the legislation until the full draft Identification Rules are published.

33. The provision for full or partial exemption from identification requirements for certain 'low-risk' services (Part 2, Division 3) is welcome in principle but should not be left to the discretion and judgement of AUSTRAC to make in Rules. We believe that the Parliament should address itself to the 'proportionality' of reporting requirements, and provide for major exemptions, in the primary legislation.

34. The provisions relating to re-verification of identity (Part 2, Division 5) are not entirely clear – but we read them as requiring re-verification even where a customer has only fairly recently been verified by the same reporting entity. This again seems unnecessary and disproportionate.

35. The requirement for reporting entities to identify beneficial owners and to try to understand the ownership and control structures of customers that are legal entities or arrangements is, in our view, an inappropriate allocation of responsibility. The same applies to the requirements in the draft Identification Rules for minimum Know Your Customer (KYC) information to include the names of all directors (of companies) and of board members (of other legal entities).

36. While APF has no brief for corporate privacy, we think the principle of 'outsourcing' official investigative functions to reporting entities is wrong. If Parliament wishes to make it harder for people to hide their business affairs behind complex legal arrangements, then surely this should be done through a combination of obligations/controls on the actions of individuals, and greater powers/resources to investigate alleged abuses. This proposal compounds the overall effect of the Bill in turning businesses into state spies.

Reporting requirements (Part 3)

37. The 'suspicious matters' reporting requirements are amongst the most pernicious aspect of the legislation. We note that the terminology has changed from 'suspicious transactions' under the FTR Act. This means that the grounds for reporting have become even more subjective. We also note that the inclusion of 'preparatory to the commission of an offence' in s.39(1)(e) appears to invite pure speculation.

38. 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.

39. 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. 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',

40. There is also a 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.

41. The 'suspicion' reporting regime cannot be divorced from the legislative prohibition on notifying the subject of the report. 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. 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.

42. We strongly urge the Government to consult indigenous and NESB community representatives about the implications of reporting suspicious appearance or behaviour.

43. If the 'suspicion' reporting requirement is to be retained in any form, it must be limited to much more objective criteria, linked clearly to the anti-money laundering and counter terrorism objectives, and expressly not linked (as the draft Bill does) to an unlimited range of offences or misdemeanours (s.39(1)(d)).

44. The proposed regime expects employees of reporting entities and their employees to be familiar not only with a huge range of domestic laws, but also with 'equivalent' offences in foreign laws (s.40). This is completely unrealistic and further illustrates the problem of effectively 'outsourcing' intelligence functions to reporting entities.

45. Given the subjective criteria for reporting (as currently set out in AUSTRAC Guidelines and to be set out in Rules (s.39(6))), it is far too onerous to make failure to report a suspicious matter a serious criminal offence (s.39(4)). This provision will inevitably lead to employees of reporting entities 'playing it safe' and over-reporting. We understand that AUSTRAC is already concerned about the level of inappropriate reporting under the FTR Act, and we suggest that the government be asked to produce statistics and other evidence of the scale and nature of this problem.

46. We note that some of the offence provisions in the Bill include a 'good faith' defence (e.g. ss.36, 46, 64) – it is not clear to us whether this applies to failure to report – s.39 appears to create a strict liability offence.

47. We note that the Bill provides for regulations to set a monetary threshold for International Funds Transfer Instructions to be reported (s.42 (1)(e)). As with the other thresholds, we support the principle but submit that it should not be left to subordinate legislation. Sensible thresholds should be set in the primary legislation.

Monitoring requirements – AML/CTF Programs (Part 7)

48. The Overview states (p.4) that the Bill would require businesses to 'monitor customers and their transactions and activities throughout the course of the business relationship'. This demonstrates more clearly than anything in the Bill itself the level of intrusion that is required.

49. It is only in the detail of the draft legislation and rules that the true extent of intrusion becomes even more obvious. Reporting entities will be required to classify every customer according to risk criteria (Draft Rule, AML/CTF Programs, paragraph 14). It is not clear if the reporting entities will be allowed to inform customers of their risk classification – we suggest that they should be *required* to do so, as well as having to respond to enquiries under National Privacy Principle 6.

50. Given that assessment as a 'higher risk' customer has the potential to adversely affect an individual, we believe that there must be a mechanism for challenging assessments. The Bill currently contains no such review mechanism.

51. We also suggest that reporting entities may well start to discriminate against 'higher risk' customers, either by declining their business or by imposing differential terms, conditions or charges. While this is not strictly a privacy issue, we recommend that the implications and fairness of this potential for discrimination be comprehensively addressed.

52. The draft AML/CTF Rules on Section 74 (AML/CTF Programs) appear to adopt a risk management approach which we would strongly support as consistent with the proportionality principle. Unlike the more general identification and reporting requirements, the AML/CTF Programs Rules focus (as does s.74 of the Bill) on money laundering and financing of terrorism offences.

53. However, this focus would appear to be undermined by the breadth of the draft Rules for AML/CTF Programs. For the purposes of reducing the risk of money-laundering and terrorism financing, it should not be necessary to routinely monitor *all* customers and *all* transactions, even if some of them will be classified as low risk. The 'floor' of *minimum KYC information* is set too low, while the *additional KYC information* and *enhanced due diligence* requirements are likely to apply to far too many customers, both as a result of the broad and subjective criteria and because of natural risk aversion by reporting entities concerned about the penalties for breaches of their obligations.

54. We note that the draft Rules for AML/CTF Programs envisage *employee due diligence* programs. This has obvious implications for employee privacy, which is currently unprotected due to the employee records exemption in the Privacy Act 1988. We submit that if the legislation either expressly or implicitly requires employee due diligence programs, then reporting entities *must* lose the exemption and be made subject to the Privacy Act for the purposes of any information held as a result of AML/CTF requirements. In practice, it would be impossible to separate this from other personnel information and the obvious solution is a complete abolition of the employee record exemption, as already recently recommended by the Senate Legal & Constitutional References Committee[3].

Countermeasures (Part 9)

55. The provision for a blanket ban on transactions with residents of prescribed countries appears disproportionate. It is difficult to envisage circumstances in which there would not continue to be perfectly innocent and harmless transactions involving any country – a blanket prohibition could have serious adverse consequences for individuals in the destination country who rely on funds transfers.

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

Record-keeping requirements (Part 10)

56. National Privacy Principle 4.2 requires private sector organisations to dispose of personal information once it is no longer needed. It would be consistent with this principle for any retention periods under this legislation to be a short as possible to fulfil the objectives. The legislation (and/or Rules) should resist the temptation to set long or indefinite retention periods simply on the basis of hypothetical utility. A limited retention period is particularly important in relation to suspicion reports which continue to be 'hidden' from the subject – at the moment, and under the proposals, a suspicion report remains on the AUSTRAC database indefinitely without the individual's knowledge, even if no action is taken against them or relevant investigations continuing – this is an intolerable denial of natural justice.

Secrecy and Access (Part 11)

Secrecy

57. Access to and correction of personal information are fundamental rights under both the Privacy and FOI Acts, and should only be limited to the minimum extent necessary to accommodate other public interests. Individuals do have access to significant and international funds transfer reports held by AUSTRAC under the FTR Act and we assume that this will continue under the proposed law. Similarly, we assume that individuals' requests for access to general AUSTRAC intelligence and analysis about them would be considered on its merits under the relevant provisions of the Privacy and FOI Acts.

58. However, as already noted above, the express secrecy of suspect transaction reports (s.95) is a major problem. We accept that there needs to be an option of withholding intelligence where giving access would prejudice an actual or potential investigation, but there can be no justification for a permanent prohibition on access and notification for all customers[4]. Even the controversial wiretap laws in the United States provide for notification after the event, and a similar requirement to notify should apply under this legislation.

59. To the extent that direct access rights do not 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

60. The secrecy provisions (s.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 Ombusdman and the IGIS), and to courts and tribunals in relation to challenges by individuals. The present drafting of ss.93-95, and 105 would appear to constrain AUSTRAC and reporting entities from cooperating with any investigations or court/tribunal proceedings brought by an aggrieved individual.

[4] It is inappropriate to use the perjorative term 'tipping off', when what is being proposed is a limitation on an individual's statutory right to be notified of uses and disclosures.

Access by agencies

61. As already explained in the introduction to this submission, the provisions in sections 98-104 open the way for a potentially unlimited range of uses of AUSTRAC information, and need 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.

62. The range of agencies and purposes for which access can be given needs to be specified in the primary legislation and not left to AUSTRAC Rules.

63. The provisions for designated agencies in receipt of AUSTRAC information to further disclose that information (s.110(3)) are far too generous, and undermine any limitations that might be implied by the references to AML/CTF offences or even to AUSTRAC purposes. Section 110(3)(a) appears to effectively allow use and onward disclosure of AUSTRAC information for *any* lawful purpose of a designated agency.

64. The Bill seeks to impose conditions on disclosure designed to protect individuals' privacy. It does this by requiring AUSTRAC to obtain assurances from state & territory, and foreign, agencies about compliance with the IPPs in the Privacy Act (s.99(2), s.103(1)(b) & (s)(b) and s.104(1)(b).

65. While we welcome this attempt to safeguard privacy, we question how effective the provisions can be given the unenforceability of any assurances given. We 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).

66. 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.

67. The Bill should also require the undertakings given by foreign governments to extend to other human rights. Important as privacy rights are, protection against arbitrary arrest and imprisonment, torture etc is even more crucial.

68. The Bill should also provide for severe penalties for any unauthorised use of AUSTRAC information (and of report information prepared for submission to AUSTRAC) – see below under offences.

Offences (Part 12)

69. We have already raised some concerns about offences under the 'Reporting requirements' heading above.

70. The proposed offences of giving false or misleading information/documents (ss.107-108) are too onerous. They should only apply where there is an intention to mislead related to some wrongdoing – i.e. provision of false information with criminal intent. Individuals should not face criminal prosecution for inadvertent provision of inconsistent information. Commonwealth agencies routinely and persistently underestimate the extent to which individuals operate lawfully with different combinations of name and address – the extent does however become apparent through the difficulty, cost and inconvenience involved in data-matching. Governments increasingly pursue identity management initiatives which fail to acknowledge the reality that many individuals have different name/address combinations in different contexts.

71. Another related provision with similar problems is s.110, which makes it an offence for a reporting entity to provide a designated service using a false customer name. We submit that it is quite unreasonable to expect reporting entities to be able to definitively detect 'false names', whatever that means. Their obligation should be limited to accepting evidence of identity to the required standard – if a customer has provided false information with criminal intent, then that should remain an offence by the individual, but not invoke any penalty for the reporting entity.

72. Section 110 also makes it an offence to provide a designated service on the basis of customer anonymity. This is a direct override of National Privacy Principle 8, and while it can be justified in relation to a 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.

73. Given the proposed changes in the regime from 'services' to 'entities', and from 'transactions' to 'matters', there is a risk that contacts between individuals and businesses which can currently be, and should remain, anonymous will become subject to identification. This would include simple enquiries about investment options and products. Insisting on individuals having to identify themselves before making even simple enquiries and 'shopping around' as wise consumers is not only excessive and objectionable in principle but would also expose them to unwanted marketing – already a major concern being addressed by DoCITA in the context of a national do-not-call register.

74. The offence provisions are currently 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.

Audit (Part 13)

75. The Bill appears to allow authorised officers to enter reporting entities' premises and exercise monitoring powers either on the authority of a monitoring warrant or with the occupier's consent. However, many of the safeguards would appear to apply only where a warrant is in force.

76. We submit that many of the same safeguards are also needed where the entry and monitoring is done 'with consent'. This is partly because the 'occupier' may not be the person whose interests are affected, but more significantly because occupiers are unlikely to fully comprehend the implications of consenting, or the actions that could follow (s.121 requires only minimal information to be given).

77. The provisions for Monitoring warrants (Part 13, Division 6) provide some safeguards, including a useful requirement for Magistrates to be satisfied that access is reasonably necessary, and to request further information in order to satisfy themselves.

78. However, the provision for the warrant issuing function to be conferred on a Magistrate in a personal capacity (s.129(1)) continues a disturbing trend. The government increasingly uses the involvement of judicial officers in Executive functions to give a misleading impression of judicial oversight. Unless judges or magistrates are exercising judicial powers, with all the requirements for natural justice and evidence based decision making that that implies, they are in reality no more than co-opted members of the Executive[5]. Also, the fact that the function is voluntary (s.129(2)) means that those magistrates performing it will by self-selection have no doubts about the legitimacy of the role, while those who may be troubled by the role confusion are likely to decline to participate. This further weakens the extent to which the warrant-issuing regime can be seen as truly independent.

[5] This is a matter currently being considered by the Security Legislation Review Committee – see http://www.ag.gov.au/agd/WWW/agdhome.nsf/AllDocs/C2CE3EBE73794EF8CA2570A5001FAB3C?OpenDocument

Information-gathering powers and Notices (Parts 14-15)

79. The relationship between the Information-gathering powers in Part 14 and the power to issue Notices (including to produce information) in Part 15 is unclear. It should be clarified so that an assessment of the privacy implications can be made.

Immunity for AUSTRAC employees (Part 15)

80. It is not clear why the immunity provided by s.155(3) does not contain the same 'in good faith/without negligence' condition as s.170.

Policy principles/directions (Part 16)

81. The relationship between s.174 and s.190 is unclear. Both appear to envisage written Ministerial directions about the exercise of AUSTRAC's functions – why are both needed?

Other General points

Verification of customer identification information

82. In order to fully assess the privacy implications of the draft Bill and Rules, 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 foreshadowed review of the case for a national identity card
- Various other identity management initiatives

83. 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.

84. 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.

Relationship between Legislation and Rules

85. In our view, too much of the detailed implementation, including many of the parameters of the scheme which give rise to concern, will be set out in AUSTRAC Rules, rather than in the legislation. While making the Rules subject to disallowance by Parliament provides some control, it is not enough. The reality (and clear intention) is that it is much easier to make changes through Rules than through legislative amendment.

86. We note that s.191 provides for binding Ministerial Directions to AUSTRAC about the making of Rules. This would appear to make the Rules in effect backdoor Regulations – we are not sure what interest is served by suggesting throughout the legislation, until s.191, that AUSTRAC would be exercising its own discretion in the making of Rules.

Consultation

87. There is no express requirement for AUSTRAC to consult with representatives of consumer interests when developing Rules and otherwise implementing the legislation. We submit that there should be specific statutory requirements for adequate and timely consultation.

Coverage and Application of Privacy Act

88. The AUSTRAC Draft Guidance paper on Applicable customer identification procedures highlights the fact that many reporting entities under the new legislation would be exempt from the *Privacy Act 1988* under the small business exemption from that Act.

89. 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. As the Guidance paper acknowledges, some customers may have privacy concerns about the protection of information collected about them by reporting entities.

90. 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. It would however be appropriate to apply the more recent private sector NPPs rather than the outdated IPPs that apply to Commonwealth agencies. This would automatically be the case if the small business exemption was removed for reporting entities.

Enforcement of Privacy Act notice requirements

91. To the extent that reporting entities are subject to the Privacy Act, they are required by NPP1.3 (or 1.5) to ensure that individuals about whom information is collected are made aware of certain matters. However, it is clear from personal experience of our members that many financial institutions are not currently meeting this obligation – customers transferring money overseas for example are often not given any information about reports to AUSTRAC.

92. The Privacy Commissioner does not have audit powers in relation to compliance with the NPPs, and can only respond to complaints. By definition there are unlikely to be complaints about a failure to give notice, and there is therefore a major problem of enforcement of these requirements.

93. To address this shortcoming, all of the following should be implemented:

- 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

March 2006

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

Contact for this submission is Nigel Waters, Policy Coordinator
02 4981 0828