

Anti-Money Laundering (AML) Reforms

Submission by the Australian Privacy Foundation

March 2004

The Australian Privacy Foundation

The Australian Privacy Foundation is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. 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

Introduction

The federal government is proposing reform to the Australian anti-money-laundering regime, ostensibly to comply with international obligations under the revised recommendations of the Financial Action Task Force on Money Laundering (FATF). Details are at www.ag.gov.au/aml. We use the word ‘ostensibly’ advisedly, as it is already clear that the existing Australian transactions reporting regime goes well beyond what is required by international agreements (including the revised FATF 40 recommendations – see the detailed analysis in the Liberty Victoria submission). We are deeply concerned that an already highly intrusive surveillance system is proposed to be massively extended for a variety of reasons, using the FATF recommendations as a convenient excuse, and without a sensible ‘risk-based’ assessment.

While we welcome the opportunity to make a submission we note that ourselves and other consumer and civil liberties groups were not specifically notified of the consultative process, despite being represented on the AUSTRAC Privacy Consultative Committee (PCC) and our interest being obvious. We take this as an indication that the review team are not yet sufficiently aware of the importance of privacy and related issues. Further evidence of this is contained in the wording of the Issue papers, which say:

“In deciding that Australia should take steps to implement the revised Forty Recommendations, the Government is mindful of two considerations:

- 1) the need to ensure that regulation does not interfere with legitimate commercial activity; and
- 2) the need to safeguard both Australian business and the Australian community from the impacts of crime.”

There is no mention of the legitimate privacy interests of all Australians which should be a major additional consideration to be balanced against the others.

While the Office of the Privacy Commissioner is apparently being consulted, there must be some doubts about how much attention it will be able to devote to the AML issue, given its serious resource pressures and consequent cutbacks in policy work, as confirmed in Senate Estimates Committee hearings and recent statements by the Commissioner.

At the very least, the government should in this instance follow the Privacy Commissioner's general recommendation for a thorough independent Privacy Impact Assessment (PIA) for all major new initiatives, so that the community can engage in a considered debate about the price it is prepared to pay for the dubious benefits of a massively expanded transaction reporting regime.

We draw attention to the 1993 report of the Senate Committee on the FTRA and AUSTRAC which includes the following warning, which is even more timely now:

“From time to time, law enforcement agencies in the proper discharge of their responsibilities seek further powers and greater jurisdiction from Government. Government should not readily grant them.

Because law enforcement mechanisms are prone to impact heavily on the life and liberty of members of the community they must, in a free and open society, be instituted only after a close analysis and with considerable caution. Other than in exceptional circumstances evidence on the basis of which they are established should be comprehensive, complete and compelling.”
(Paragraphs 11.26 & 11.27)

The Committee went on to recommend a further review of the FTRA after three years. While the government accepted this recommendation it has not been implemented. The current review at least belatedly gives the community the opportunity to re-examine the justification for one of the most intrusive yet least well known elements in the law enforcement infrastructure.

The Proposal

It is proposed to repeal the Financial Transaction Reports Act 1988 and replace it with a completely new anti-money laundering law. Amendments to the FTRA will apparently not suffice because of the wider scope required to meet the recommendations and consequential need for a wider constitutional basis.

The wider scope is partly due to the growth of electronic non-face-to-face transactions but also confirms the ‘function creep’ that has occurred with the FTRA and its implementing agency AUSTRAC over the last 15 years. The customer due diligence (CDD or ‘know your customer’), record-keeping and reporting requirements will be extended to a much wider range of industry sectors – essentially anyone involved in

actual or prospective transfers of value. This will bring in real estate agents, various dealers, accountants, lawyers and notaries etc, as well as the existing 'cash dealers' (financial institutions, casinos, bookmakers).

The range of offences to which suspect transaction reporting is linked may change. The objectives of the new law will expressly include combating of terrorist financing as well as money-laundering, which inevitably makes it more difficult to maintain thresholds – both of type of offence and monetary amounts. Thus the way is opened to ever-increasing levels of surveillance on the basis that even small exchanges of value, unconnected with any other offence, can contribute to terrorist financing.

Compliance costs and problems

Industry representatives involved in the consultation forums were understandably concerned about potential compliance costs, but there was also some recognition of privacy issues and how these might affect levels of trust. Also mentioned was the potential for excluding low value individuals from some services – if the costs of CDD and ongoing record keeping become too great institutions could decide it is not commercially viable to service clients with only modest income/assets.

It is not clear how the CDD requirements could sensibly operate in the context of some real estate and other transactions such as those concluded through auctions, where contract need to be formed without any prior evidence of identity.

Another problem is the potential conflict between an obligation to seek more information from some customers vs the obligation not to tip off anyone suspected. Industry representatives were also concerned about the enforcement/penalties regime – they will demand indemnity for employees and organisations reporting in good faith, although this removes the disincentive for over-reporting. The government appears to be leaning towards either criminal sanctions or civil penalties with a criminal standard of proof (as recommended by the ALRC) for failure to meet obligations under the new law. Significant penalties will inevitably encourage 'over-zealous' CDD, record-keeping and reporting.

Proposal fails proportionality test

While the Issue papers pay lip service to risk management, there seems to be no recognition that a proper risk assessment might lead to the conclusion that imposing requirements on thousands of small businesses might not be justified as a proportionate response to an imperfectly specified and quantified risk. There is no hard evidence given in the documentation about the incidence of organised crime or terrorists using 'soft' transactions in pursuit of their activities – just generalised allegations.

Even if there is evidence, it is not clear why these transactions cannot be picked up at other stages eg: in property title changes or the interaction with the mainstream financial systems. The review team seem to be proceeding on the assumption that the FATF recommendations require a comprehensive CDD and reporting regime that has few thresholds or limits, but instead applies to all 'value transfer' relationships. While some of the issues papers canvass suggestions as to thresholds, and scope for exercising discretion, the starting point appears to be to apply the requirements to *all* transactions, with industry groups having to justify any suggested exclusions.

Probably the most controversial, and objectionable, extension of the regime is into real estate. Extending evidence of identity requirements into property transactions and even enquiries would be a major contradiction of the anonymity principle in the Privacy Act (NPP8). Currently, accurate identification only comes into play in conveyancing – involving lawyers not real estate agents. Requiring realtors to demand 'evidence of identity' (EOI), potentially even for enquiries about rentals, would be a massive intrusion into privacy. We are concerned that the real estate industry may not have woken up to the implications of the proposals, and urge the government to ensure that their reaction is specifically canvassed before drafting the legislation.

Evidence of Identity a wider and more complex issue

It is not yet decided whether specification of required ID particulars (whatever replaces the current 'points' test) will be in legislation, regulations or left to discretion. It is however essential that any decisions are made in a wider context of a debate about authentication and identification standards for different purposes. The AML reform is only one of a number of initiatives in which the question of EOI is arising, but could well be an early driver of decisions. There was casual mention in one consultation forum of use of tax file numbers (TFNs) although it was pointed out that there were major problems with TFN integrity. It may well be that no current or prospective ID documents are good enough to support the CDD requirements being considered, and we question whether there is any point in having a CDD regime that would be let down by inadequate EOI.

Major new record retention requirements

As well as initial EOI, the new regime will also impose new *ongoing* CDD and record keeping requirements. For instance, the Real Estate Sector Issues paper, for example, says:

“The new FATF standards will require the collection and retention of additional customer due diligence information relevant to ongoing due diligence measures. Such information might include transaction information and business correspondence. This information will need to be kept in a consistent format to allow ready access by regulatory agencies.

While the current FTR Act requires document retention for seven years, consideration will be given to reducing the period to five years from the close of the business relationship, consistent with the record retention provisions of the *Proceeds of Crime Act 2002*.”

While reducing the retention period sounds like a concession, it is not in practice – the financial institutions currently covered by the FTRA have to keep records under other legal requirements (probably still for at least seven years). What is meant in practice is a completely *new* requirement for organisations such as real estate agents to collect and keep new records for five years.

Suspect transaction reporting inherently flawed

The suspect transaction reporting requirements are in some ways the most objectionable aspect of the existing and proposed regimes. Unlike some of the other requirements there are no ‘thresholds’ and only limited guidance on criteria for suspicion. The result is that, already, junior staff in financial institutions are under a legal obligation to exercise judgments that could result in a secret file about any one of us. It is well known that senior staff filter out some reports that are obviously not well-founded, but how many more are going through to the AUSTRAC database where they are kept indefinitely and accessible to more than 25 different agencies, to make of what they will.

The whole principle of permanent and secret records, with potentially adverse consequences for individuals, based on ‘lay’ interpretations of vague guidelines, is anathema to a civilized society, and directly contrary to the objectives of Privacy and Freedom of Information laws.

The unacceptable characteristics of suspect transactions reporting will be seriously compounded if reporting obligations are extended, as proposed, to real estate agents and jewelers. At least financial institutions can be expected to have minimum standards of staff training and to employ experienced senior staff to oversight the reporting. Neither of these is realistic for the thousands of small businesses that would be covered by the new law.

Proposal must be cut back

We accept that there is a public interest in an effective *significant* transaction monitoring system to combat money-laundering, and that this may, subject to rigorous safeguards, outweigh highly prized privacy rights, even in relation to sensitive financial affairs. But the current FTRA regime goes well beyond this into routine monitoring of even tiny transactions (if they cross borders) and highly subjective and intrusive suspect transaction reporting.

The proposed new legislation would significantly compound the problems with the existing regime. In almost every respect, the new law would result in more intrusion for more purposes and with fewer constraints, for unsubstantiated benefits.

Before any new requirements are introduced, the government must outline the incidence and scale of the criminal activity which the laws are purported to address. It should also explain more persuasively, if it can, how the extreme levels of surveillance proposed would assist significantly in combating that activity. A proper cost:benefit analysis, including a comprehensive Privacy Impact Assessment, is essential.

Australian Privacy Foundation
19 March 2004

Contact:

Nigel Waters, Board Member
Australian Privacy Foundation
<http://www.privacy.org.au>
Tel: (02) 4981 0828 or Mobile: 0407 230 342
Fax: (02) 4981 0995
nigelwaters@iprimus.com.au
