Senate Legal and Constitutional Affairs Committee Inquiry into the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 and associated legislation

Additional comments and information from the Office of the Privacy Commissioner arising from the Office's attendance at the Committee's inquiry on Wednesday 22 November 2006 and from an additional question forwarded from the Committee on Thursday 23 November 2006.

Response to three questions from Senator Ludwig:

Use of the Electoral Roll:
The electoral roll contains information about the vast majority of adult citizens. Generally speaking, individuals have no choice about whether to provide the information and little choice about its publication, and as such, individuals have an expectation that this information will only be used for the purpose for which it was collected.

The primary purpose for collecting personal information for inclusion in the Electoral Roll is to produce and maintain an accurate record of those who are entitled to participate in the electoral process, thus minimising electoral fraud and promoting the valid and lawful participation of all eligible citizens in the democratic process.

In light of this, the Office considers that, unless there is a very strong public interest to the contrary, the collection and use of personal information on the electoral roll should be restricted to the primary purpose for which the register is set up and for which the information is made public. The gradual expansion of uses to which this information may be applied risks undermining the community's trust in the handling of electoral information.

Although the electoral roll is currently used for verification of identity for the purpose of monitoring of financial transactions under the *Financial Transaction Reports Act 1988* the significant extension of the number of organisations which will be reporting entities under the AML/CTF Act, compared to the Financial Transaction Reporting legislation, will inevitably result in a much wider range of organisations having cause to verify identity by reference to the electoral roll.

Consideration should be given to ensuring that only as much information as is absolutely necessary is provided from the electoral roll to organisations provided access by virtue of the AML/CTF regime and that strong protections are in place to prevent unauthorised or further use being made of the information.

Suspicious Transactions:
The *Financial Transaction Reports Act 1988* currently requires reporting entities to pass on details of suspicious *transactions* to AUSTRAC.[1] The proposed provisions are far broader, capturing more communications beyond actual transactions.

[1] Section 16

The Office is concerned that these provisions may induce over-reporting by entities, given that the Bill makes it a criminal offence not to report suspicious matters. As a result, it is reasonably foreseeable that large volumes of individual's private information may flow to AUSTRAC unnecessarily.

The Bill in its present form significantly expands the range of agencies which will have access to AUSTRAC's information, without giving the individuals concerned rights to access their personal information, and correct information where it is inaccurate. The Office suggests that the discretion regarding disclosures to agencies should be narrowed. The Bill should provide that suspect matter information may only be used and disclosed for anti-terrorism and counter-terrorism financing or other serious offences.

Regarding individual rights of access, the Office recognises the need for secrecy surrounding reporting to avoid compromising investigations. However, given the volume and diversity of information collected, it is reasonable to suppose that not all suspicious matter reports will be actioned by AUSTRAC. In this case, there seems to be a sound case for allowing individual's access to information after a set period where no further action has been taken.

Privacy Impact Assessment

Question: What is OPC's assessment of the recommendations made in the Privacy Impact Assessment[2] that have not been accepted by the Government[3], particularly in regard to those it deems of most significance.

Answer: Of the recommendations in the Privacy Impact Assessment that the government has not accepted the Office believes the following three are of most significance:

51. That the threshold for significant cash transaction reports be increased to $16,000, by amending the definition of 'threshold transaction' in cl 5 of the Bill. (See also Recommendation 18 in relation to also indexing values every five years.)

The Office believes that the general thrust of recommendation 51 would assist in reducing the amount of personal information collected unnecessarily.

In each of four submissions made during development of the Bill, the Office has recommended that the significant transaction threshold be raised. Most recently, in its submission to the Committee, the Office has noted (at page 6):

> "There has been no adjustment to the threshold in the 18 years since the FTR Act was introduced. In the Office's view, the current process of regulatory reform provides an opportunity for this threshold to be revised upward. As

[2] The PIA can be found at: http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(85861BE64F280B2D8725056734D25146)~PIA.pdf/$file/PIA.pdf

[3] The Government's response can be found at: http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(85861BE64F280B2D8725056734D25146)~PIS.pdf/$file/PIS.pdf

organisations will already been undergoing changes to their compliance processes and systems to accommodate the proposed regulatory reform, it seems opportune to amend this threshold amount to a more appropriate figure. Once organisations have completed the process of establishing processes to meet the new regulatory arrangements, they may be highly reluctant to support a change in the threshold amount in the foreseeable future."

62. That AUSTRAC limit online access to its databases to the following agencies: Customs, Australian Security Intelligence Organisation (ASIO), the Australian Federal Police (AFP) and State and Territory police forces, the Australian Crime Commission (ACC) and State and Territory crime commissions, the Australian Taxation Office (ATO), and State and Territory revenue agencies. Therefore no online access should be allowed to: Australian Commission for Law Enforcement Integrity (ACLEI) and its State equivalents, Australian Competition and Consumer Commission (ACCC), Australian Prudential Regulation Authority (APRA), Australian Securities and Investment Commission (ASIC), Centrelink, the Child Support Agency, ad-hoc royal commissions, or any other recipient agencies added by regulation.

In regard to recommendation 62, the Office has expressed no view on which specific agencies should be afforded online access to the AUSTRAC database. The Office reiterates its previously expressed view that access to personal information held by AUSTRAC should be narrowly restricted to those agencies and other bodies that require such information as a necessary part of responding to major crimes, such as money-laundering or terrorist financing.

The Office has also recommended that the issue of extending access to the database to new agencies be considered separately from the broader reform process.

77. That sub-cl 99(3) be amended so that each State or Territory Government partner agency must either: • demonstrate to AUSTRAC that all their activities are subject to a statutory scheme which sets out privacy principles, includes independent oversight by a Privacy Commissioner (or equivalent), and enables a complainant to obtain an enforceable remedy from an independent body for any harm suffered as a result of breaching one or more of the privacy principles, or • undertake to comply with the IPPs in the Privacy Act, and submit to the jurisdiction of the Australian Privacy Commissioner. [Note sub-cl 99(3) as referred to above is equivalent to sub-cl 126(3) of the final Bill]

In regard to recommendation 77, the Office has consistently recommended that measures be progressed to ensure that individuals have enforceable privacy rights if their personal information is disclosed by AUSTRAC to state government bodies beyond the jurisdiction of the Privacy Act.

Other recommendations:

13. That Rule 2.2.14 be amended to delete the requirement to check a person's credit bureau history for the purposes of customer verification when using e-verification.

In regard to recommendation 13, the Office recommends paragraph 2.2.14 of the Rules be re-drafted to clearly indicate its intent and effect, and prevent the rule from being interpreted as authorising or requiring the disclosure of consumer credit reports in an expanded range of circumstances.

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

15. That the definition of 'designated services' in the Bill be amended to exclude all services which involve a one-off transaction under a threshold of $1,000.

In regard to recommendation 15, the Office has no view on the specific threshold.

However, in its submission to the Attorney-General's Department on the second exposure draft of the Bill (August 2006), the Office (at page 6) made the general comment that:

> "The Office encourages the Department to consider setting some threshold for these transactions, so that only those of significant value trigger reporting obligations."

Similarly, the Office supports the general thrust of recommendations 18 that threshold amounts should be subject to periodic increase.

30. That AUSTRAC work with industry and public interest representatives to devise model, layered privacy notices for reporting entities to use. The model notices must include alternatives depending on whether the service requested is considered low, medium or high ML/TF risk, and include alternatives for use with children, people of non-English speaking background, and people with decision-making disabilities.

The Office would generally support recommendation 30.

Under National Privacy Principle 5, organisations must set out in a document clearly expressed policies on its management of personal information. In recognition that some individuals may find privacy notices long and difficult to read, the Office encourages the use of "layered" privacy notices. Such notices are an effective means of communicating the personal information handling practices of an agency or organisation.

While layered privacy notices are not required by the Privacy Act, the Office has previously submitted[4], in regard to the Bill, that:

> "In recognition of the pervasiveness of the scheme, these protections could, in some places, afford a higher standard of protection than those offered by the Privacy Act, including by limiting the number of exceptions to a use or disclosure provision. Such an approach is in place for the handling of credit

[4] See Submission to the Attorney-General's Department on the exposure draft of the Bill, paragraph 50.

> reporting information, Medicare and PBS claims information, and Tax File Numbers.[5]"

35. That the Bill prohibit any use of personal information collected under the KYC requirements for marketing purposes, except on an 'opt in' basis.

The Office would support recommendation 35. This is consistent with its view that additional protections should be afforded to information collected pursuant to the Bill.

It should be noted that National Privacy Principle 2.1(c) permits personal information, other than sensitive information, to be used or disclosed for direct marketing subject to certain provisions being met. One provision is that the individual be afforded the opportunity to "opt out" from receiving the direct marketing.

Accordingly, the application of the Privacy Act to reporting entities would not address recommendation 35. As noted above, the Office's has previously expressed the view that, in some places, protections in addition to the Privacy Act may be warranted.

The comments made above concerning recommendation 35 apply similarly to recommendation 39 (regarding the *disclosure* of KYC information for direct marketing).

40. That the Bill prohibit any disclosure of personal information collected under the employee due diligence requirements, except as required by this or another statute or court order, where necessary to prevent or lessen a serious and imminent threat to any person, where necessary for law enforcement purposes, or with the person's consent.

Under section 7B(3), employee records held by organisations about individuals are exempt from the Privacy Act.

Accordingly, subjecting reporting entities to the Privacy Act would not address recommendation 40.

46. That Rule 8.2 (AML/CTF risk awareness training program) be amended to include privacy responsibilities and risks.

The Office would generally support recommendation 46.

In its April 2006 submission to the Attorney-General's Department on the first exposure draft of the Bill, the Office (at paragraph 104) suggested:

> 104. The Office also suggests that the Rules for AML/CTF Programs include requirements for reporting entities to take reasonable steps to ensure that employees and agents are aware of obligations concerning the appropriate handling of personal information collected under the AML/CTF legislation. This could, for example, be expressly provided for in rule 26, which requires

[5] See, respectively, Part IIIA of the Privacy Act, section 135AA of the *National Health Act 1953* and Division 4 of the Privacy Act.

reporting entities to give appropriate training to employees on various matters relevant to the implementation of the Exposure Bill.

55. That paragraph 39(1)(f)(v) of the Bill be amended to require some element of 'serious crime' in the scope of offences against Commonwealth, State or Territory law, in relation to which a suspicion may be formed. 'Serious crime' should be defined in the Bill. [Note paragraph 39(1)(f)(v) as referred to above is equivalent to paragraph 41(f)(v) of the final Bill]

The Office would support the underlying theme of recommendation 59 to ensure that the regulatory regime remains focused on genuinely "serious crime."

The response would seem to suggest that *any* matter subject to an investigation and prosecution is, by that fact, a serious crime. The Office suggests that this interpretation may not accord with community expectations of what constitutes a serious crime.

82. That the Bill require recipient agencies to destroy or de-identify personal information they collect from AUSTRAC once it is no longer needed for its intended purpose. (However note that if Recommendation 77 is adopted, this Recommendation is not required.)

In regard to recommendation 82, Australian Government agencies are required to comply with the Information Privacy Principles prescribed in section 14 of the Privacy Act. These principles do not set out an obligation on agencies to destroy or de-identify personal information once it is no longer needed for its intended purposes.

Accordingly, the Privacy Act would not satisfy recommendation 82 as suggested in the first sentence of the response.

84. That AUSTRAC work with industry and public interest representatives to devise appropriate guidelines for reporting entities on: • how they should maintain appropriate data security_• how they should check the accuracy of information before use—with particular attention paid to confirming the accuracy of information before a suspicious matters report is made to AUSTRAC • how they should ensure the provision of access and correction rights, including reasonable costs and expected timeframes, and • how they should ensure the secure disposal of KYC, CDD and reporting records

The Office would support recommendation 84 as an useful way of promoting certainty and consistency regarding how personal information may be handled.

The Office also notes that the underlying intent of recommendation 84 appears similar to recommendation 85, the latter of which has been accepted.

Additional information:
In relation to the statements made to the inquiry at our appearance on Wednesday 22nd November 2006 about our Office's interaction with the Privacy Impact Assessment process the Office would like to clarify that as well as our interactions with the Attorney General's Department a consultation meeting to discuss our public submissions on the AML/CTF exposure drafts was held on 28th August 2006 with the consultant undertaking the PIA.

Question from Senator Payne on 23 November 2006

Question: What is OPC's view of the submission from Baycorp Advantage (No.22) at pages 6-7 regarding a proposed amendment to Part 3A of the Privacy Act?

Answer: The Attorney General's Department is responsible for amendments to the Privacy Act. However, this Office does not believe that the Bill as currently drafted specifically requires the amendments suggested by Baycorp Advantage. The Australian Law Reform Commission will be considering the credit reporting provisions as part of its wider inquiry into the Privacy Act. That inquiry would be a more appropriate vehicle in which to canvass the issues raised by Baycorp Advantage.