Australian Government
Office of the Australian Information Commissioner

Julie Dennett
Committee Secretary
Senate Standing Committees on Legal and Constitutional Affairs
PO Box 6100
Parliament House
Canberra ACT 2600

Dear Ms Dennett

Combating the Financing of People Smuggling and Other Measures Bill 2011

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to make a submission to the Senate Standing Committee on Legal and Constitutional Affairs on the inquiry into the *Combating the Financing of People Smuggling and Other Measures Bill 2011* (the Bill).[1] My Office is the national privacy regulator for personal information under the *Privacy Act 1988* (Privacy Act) and also has responsibilities for freedom of information and information policy across the Australian Government.

The Purpose of the Bill

The OAIC understands that the purpose of the Bill is to amend the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), the *Financial Transaction Reports Act 1988* (FTR Act) and the Privacy Act in order to:

1. introduce a more comprehensive regulatory regime for the remittance sector to combat money laundering and terrorism financing[2]

2. introduce measures for information sharing of financial intelligence information prepared by the Australian Transaction Reports and Analysis Centre (AUSTRAC)[3]

3. enable reporting entities under the AML/CTF Act to use limited (identifying) personal information held on an individual's credit information file for the purposes of electronic verification of customer identity (e-verification)[4]

4. enable the AUSTRAC Chief Executive Officer to exempt cash dealers from obligations under the FTR Act in the same way in which the AUSTRAC CEO can do so under the AML/CTF Act.[5]

This submission focuses on the privacy aspects of Schedules 2 and 3 of the draft Bill which, respectively, relate to information sharing of financial intelligence, and e-verification of identity involving the credit reporting system.

[1] The Bill and the explanatory memorandum can be accessed at: www.parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbillhome%2Fr4509%22
[2] The Bill, Schedule 1
[3] Schedule 2
[4] Schedule 3
[5] Schedule 4

Background

The OAIC welcomed the Attorney-General's Department's (AGD) consultation on the development of the Bill. The Office provided comments on a number of occasions, including comments on the exposure draft of the Bill.[6] The OAIC also welcomes the consultation on, and publication of, AGD's Privacy Impact Assessment (PIA) on e-verification. [7] In the context of the e-verification measures, the current Bill addresses or adopts most of our prior comments and suggestions (see discussion on Schedule 3 below).

The OAIC understands that Schedule 2 is a new addition to the Bill and was not included in the public consultation for the exposure draft version of the Bill. As the additional scope for information sharing is significant, and the timeframe for the Senate Committee process is limited, it is suggested that this policy addition could have benefited from further explanation and scrutiny earlier in the process.

Schedule 2 – Amendments relating to designated agencies

Schedule 2 of the Bill amends the AML/CTF Act to expand the list of designated agencies with which AUSTRAC can share financial intelligence information (we understand this would include personal information). The Bill will enable AUSTRAC to share financial intelligence information with the Department of Foreign Affairs and Trade (DFAT), the Defence Imagery and Geospatial Organisation (DIGO), Defence Intelligence Organisation (DIO), Defence Signals Directorate (DSD), and the Office of National Assessment (ONA).

The explanatory memorandum explains that these are key agencies within the Australian Intelligence Community (AIC) and with DFAT having responsibility for administering Australia's sanctions regime, AUSTRAC's inability to share with these agencies is a barrier to achieving a holistic national intelligence effort on issues relating to people smuggling, money laundering and terrorism financing.[8]

The application of the Privacy Act to those Australian government agencies referred to in the Bill varies.[9] The proposed sharing of information between AUSTRAC and DFAT would need to comply with the requirements of the Information Privacy Principles (IPPs). IPP 11 sets out the circumstances when an agency may disclose personal information to another agency, such as if the disclosure is required or authorised by or under law or for certain law enforcement reasons.[10]

The acts and practices of the AIC agencies, such as the ONA, DIO, DIGO and DSD are exempt from the Privacy Act.[11] Accordingly, any personal information collected, used or disclosed by

[6] The previous exposure draft legislation for this Bill is available at: www.ag.gov.au/www/agd/agd.nsf/Page/Anti-money_laundering

[7] The external privacy impact assessment (PIA) was finalised in October 2009 and is available at www.ag.gov.au/www/agd/agd.nsf/Page/Anti-money_laundering, as at 9/3/2011.

[8] Explanatory memorandum, p.3

[9] The Information Privacy Principles (IPPs) in section 14 of the Privacy Act regulate the personal information handling practices of Australian Government, ACT, and Norfolk Island agencies including those with enforcement and regulatory functions. The IPPs can be accessed via the following link: http://www.privacy.gov.au/law/act/ipp

[10] IPP 11.1(d) and (e)

[11] Section 7(2) of the Privacy Act.

these agencies when fulfilling their functions is not covered by the Privacy Act.[12] In addition, an act or practice so far as it involves the disclosure of personal information to the DSD is exempt from the Privacy Act.[13]

The Bill's explanatory memorandum notes that oversight of the AIC agencies is undertaken by the Inspector-General of Intelligence and Security (IGIS), which reports annually on intelligence agencies' AUSTRAC access compliance.[14] The Bill includes certain safeguards for the disclosure of AUSTRAC information by AIC agencies, for example providing for IGIS' oversight of AUSTRAC access compliance by DIGO, DIO, DSD and ONA.[15] As we understand it, there is less prescription on the limits or circumstances of collection by AIC agencies.

In addition to IGIS oversight, the Committee could also consider the possibility of whether an appropriate privacy framework should be put in place, to support the information sharing arrangements set out in Schedule 2 of the Bill. Due to time constraints, the OAIC has not at this stage canvassed these issues with relevant agencies such as IGIS and AUSTRAC. AUSTRAC may already have such measures in place for existing information sharing arrangements under the AML/CTF Act, which could be extended and adapted to apply to the agencies referred to in the Bill.

The OAIC suggests a suitable framework could include the development of memoranda of understanding between participating agencies that clearly specify the nature, scope and limits of the information sharing activities, including what protections are afforded to any personal information collected, used or disclosed under the information sharing arrangements.

Furthermore, the framework could refer to relevant AIC agency guidelines on personal information handling practices relating to the accuracy, storage, security, retention and destruction of personal information. Where appropriate, these could be developed with the assistance of the OAIC or IGIS, with appropriate resourcing. The framework could also include a statutory review mechanism that would allow the operation of the information sharing arrangements to be reviewed and assessed after a period of time.

In the OAIC's view, such measures may assist these types of information sharing proposals by enhancing accountability and improving transparency and public confidence in personal information handling processes.[16]

The OAIC's overall position is to ensure the proposed amendments contained in Schedule 2 of the Bill only apply in circumstances where it is necessary and proportionate to facilitate personal information sharing between intelligence and law enforcement agencies undertaking their legitimate functions. The '4A Framework' developed by the former Office of the Privacy Commissioner (see Attachment A) may be of some assistance in that process.

---

[12] See section 7(1)(f) of the Privacy Act - Australian Government agencies or organisations that engage in an act or practice related to a record that has originated with, or has been received from, these agencies are also exempt from the operation of the Privacy Act.
[13] See section 7(1A) of the Privacy Act.
[14] Explanatory memorandum, p.110
[15] Explanatory memorandum, p.110
[16] See OAIC submission to Senate Legal and Constitutional Affairs Committee on the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010 (Nov 2010) available at: http://www.privacy.gov.au/materials/types/submissions/view/7153#_ftn3

Schedule 3 – Electronic verification of identity using the credit reporting system

As noted above, the OAIC welcomes the inclusion of a range of protections raised in previous consultations that will enhance the e-verification process from a privacy perspective. These include:

- adequate safeguards to protect personal information such as individual choice and control; adequate notice; limits on disclosure, use and retention of information; and appropriate sanctions for mishandling personal information. Noting that the personal information in the credit reporting system is collected and held for other purposes (the assessment of individuals' eligibility for credit by credit providers), such protections balance the expanded use of personal information.

- a note under sections 13 and 13A of the Privacy Act making it clear that a breach of the provisions in Schedule 2 of the Bill are an interference with privacy under the Privacy Act 1988

- the explanatory memorandum has been updated to refer to the Australian Information Commissioner

- offences under proposed s 35K which relates to unauthorised use or disclosure of verification information, will apply to all persons, not just those that are a credit reporting agency or a reporting entity

- a breach of proposed ss 35E and 35F (which deal with retention and destruction of verification information) will constitute an interference with privacy which may be the subject of a complaint under s 36 of the Privacy Act.

In addition to welcoming this series of measures, this submission also makes several suggestions below that the OAIC believes would improve the privacy protections within the draft Bill.

Method for credit reporting agencies' (CRAs) information matching and response

In order to limit personal information flows the OAIC generally prefers 'yes/no' (or 'challenge/ response') confirmations of the relevant personal information in processes such as those being proposed for e-verification. However, the OAIC understands that this has been considered in the present context and that the potentially high rates of 'minor' errors and the ability to protect the system from fraud may mean that a scoring system is more appropriate than a 'yes/no' response model in this case.[17]

Resolving mismatches

The OAIC notes that inaccuracies on a credit information file, such as the misspelling of an individual's name, could return a low match score which reflects negatively on an individual's relationship with the reporting entity. However, the mismatch may have been

[17] Paragraph 35B(2) of the Bill limits the information that a CRA may provide to a reporting entity as part of an assessment in response to a verification request. The OAIC understands this is likely to mean the assessment will contain an aggregate score, or ranking, which reflects the extent of the match across all fields of personal information that were checked (name, date of birth and address).

caused due to an error on the credit reporting system rather than an indication of fraudulent activity.

The OAIC suggests that the Bill could more explicitly refer individuals to appropriate dispute resolution processes to resolve claims that there was not a sufficient match in an e-verification process (that is, there was a mismatch of some information). This could link into paragraph 35C of the Bill, which requires notification of unsuccessful matches. For example, in addition to this requirement, notification could include a reference that CRAs have certain obligations relating to data quality, access and correction and that the individual may wish to seek a correction by the CRA under the Privacy Act.

Oversight mechanisms

To supplement the proposed safeguards and ensure good governance, appropriate oversight mechanisms should be in place to monitor the handling of credit information for e-verification. This is particularly relevant given the considerable period of retention of information about verification requests specified in the draft Bill. Under ss 35E and 35F CRAs and reporting entities must retain verification request information for 7 years.

For example, oversight mechanisms could include some combination of the following:

- The OAIC's existing power to undertake audits in the credit reporting sector could be expanded to monitor compliance by reporting entities and CRAs with the draft Bill's requirements (the OAIC notes that such an expansion would have resourcing implications for this Office).
- CRAs could be required to report any misuse or non-compliance by reporting entities (such as not obtaining the individual's consent for e-verification), and to suspend or cancel e-verification subscriber agreements as appropriate
- CRAs could be required to submit an annual report to the OAIC regarding the number and form of e-verification disclosures made, and the storage and destruction mechanisms in place to protect the information
- The operation of the e-verification amendments and system could be subject to the review of the AML/CTF Act's operation in 2013.

The most appropriate form and location of such oversight mechanisms may be a matter for the Committee's consideration.

Yours sincerely

Professor John McMillan
Australian Information Commissioner

11 March 2011

Attachment A:

Framework for assessing and implementing new law enforcement and national security powers

This is a framework for assessing and implementing new law enforcement and national security powers. It sets out a life cycle approach to such proposals from development through implementation to review. The aim of the framework is to bring balance and perspective to the assessment of proposals for law enforcement or national security measures with significant effects on privacy.

- First, careful analysis is needed in the development phase to ensure that the proposed measure is necessary, effective, proportional, the least privacy invasive option and consistent with community expectations. This analysis should involve consideration of the size, scope and likely longevity of the problem, as well as the range of possible solutions, including less privacy invasive alternatives. The impact on privacy of the proposed solution should be analysed and critical consideration given to whether the measure is proportional to the risk.
- Second, the authority by which the measure is implemented should be appropriate to its privacy implications. Where there is likely to be a significant impact on privacy, the power should be conferred expressly by statute subject to objective criteria. Generally, the authority to exercise intrusive powers should be dependent on special judicial authorisation. Intrusive activities should be authorised by an appropriately senior officer.
- Third, implementation of the measure should be transparent and ensure accountability. Accountability processes should include independent complaint handling, monitoring, independent audit, and reporting and oversight powers commensurate with the intrusiveness of the measures.
- Finally, there should be periodic appraisal of the measure to assess costs and benefits. Measures that are no longer necessary should be removed and unintended or undesirable consequences rectified. Mechanisms to ensure such periodic review should be built into the development of the measure. This could involve a sunset clause or parliamentary review after a fixed period.

In summary:

Analysis – Is there a problem? Is the solution proportional to the problem? Is it the least privacy invasive solution to the problem? Is it in line with community expectations?
Authority – Under what circumstances will the organisation be able to exercise its powers and who will authorise their use?
Accountability – What are the safeguards? Who is auditing the system? How are complaints handled? Are the reporting mechanisms adequate? And how is the system working?
Appraisal – Are there built in review mechanisms? Has the measure delivered what it promised and at what cost and benefit?
