Australian Government
Office of the Australian Information Commissioner

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Committee Secretary

Submission by the Australian Privacy Commissioner on the Inquiry into the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014

As the Australian Privacy Commissioner (the Commissioner), I thank the Joint Committee on Intelligence and Security (the Joint Committee) for the opportunity to comment on the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill 2014* (the Bill). I note that many of the measures proposed in the Bill have the potential to impact upon the privacy of individuals.

I recognise that the intention of the Bill is to strengthen and improve Australia's counter-terrorism legislative framework. Further, I appreciate that ensuring Australian law enforcement agencies have access to the tools and information necessary to perform their national security functions is critical to achieving this intention. At the same time, I consider that it is important to ensure that any proposals to expand the powers of those agencies accord with contemporary community expectations, including expectations about the handling of personal information.

The Committee will be aware, that the Statement of Compatibility with Human Rights (the Statement) that accompanies the Bill recognises the privacy impacts of the Bill. Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR) provides that no-one shall be subjected to arbitrary or unlawful interference with their privacy. To the extent that there is a restriction on an individual's right to privacy, any interference must be reasonable, necessary and proportionate.

In line with Article 17 of the ICCPR, Australia's *Privacy Act 1988* (the Privacy Act), recognises that the protection of individuals' privacy, through the protection of their personal information, cannot be an absolute right. Rather, those interests must be balanced with the broader interest of the community in ensuring that entities are able to carry out their legitimate functions and activities. However, where handling of individuals' personal information is authorised in the broader interests of the community (including upholding national security) it is important that those activities are accompanied by an appropriate level of privacy safeguards and accountability.

The Statement addresses these issues and sets out the existing and proposed safeguards to address privacy impacts. I have reviewed the Statement and the Bill and in the time allowed I make the following comments for the Joint Committee's consideration. In particular, I seek to advise the Committee on how the Privacy Act would interact with the Bill, and to provide my analysis of certain personal information handling practices.

General Comments

Application of the Privacy Act

The starting position is that generally Australian government agencies affected by the amendments proposed in the Bill are required to comply with the Australian Privacy Principles (APPs) contained in the Privacy Act when handling personal information, including personal information collected for the purpose of upholding Australia's national security (for example the Australian Federal Police (AFP), the Australian Transaction Analysis Centre (AUSTRAC), the Department of Immigration and Border Protection (DIBP) and the Attorney General's Department (AGD)). The exception is the intelligence agencies which are not within the jurisdiction of the Privacy Act, but are subject to other oversight mechanisms.

The APPs are legally binding principles which set out standards, rights and obligations in relation to the collection, use, disclosure, holding and access to 'personal information', that is, information or opinion about a reasonably identifiable individual. The APPs apply to most Australian government agencies and most private sector organisations and replace the former Information Privacy Principles (that applied to Australian government agencies) and National Privacy Principles (that applied to private sector organisations). I am responsible for ensuring compliance with the APPs and other obligations contained in the Privacy Act.

The APPs require that an Australian government agency only collect information that is reasonably necessary for, or directly related to, the agency's functions and activities. Further, that those agencies only use and disclose that personal information for the purpose for which the information was collected unless an exception applies to permit the information to be used or disclosed for a secondary purpose. Importantly, those exceptions include where the use or disclosure is authorised or required by an Australian law or court/tribunal order.

I note that many of the measures proposed in the Bill involve the handling of individuals' personal information. Importantly, where the proposed measures in the Bill authorise the collection, use or disclosure of personal information, this brings the activity within the 'authorised or required by law' exceptions in the APPs, to permit the collection, use or disclosure without contravening the Privacy Act. However, even where a particular collection, use or disclosure is authorised by law, the relevant agency must still comply with other obligations contained in the APPs when handling the information (including those relating to providing notice and ensuring the quality and security of the information). Further, where the Bill authorises the collection of personal information, in some instances it limits the purposes for which that information may be used or disclosed, and creates corresponding offences for unauthorised uses or disclosures of that information. Given that certain provisions of the Bill will mean that the Privacy Act does not apply to some activities as they will be 'authorised or required by law', these additional safeguards are necessary and appropriate.

These additional safeguards will complement existing measures, which include regulatory oversight by the Independent National Security Legislation Monitor, the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman. In addition, I have a range of powers under the Privacy Act to ensure that agencies are complying with their obligations where they arise under the APPs. These powers include the power to conduct assessments (previously referred to as audits) of agencies and organisations to ascertain whether personal information is being maintained and handled in accordance with the APPs, initiate investigations of matters involving the handling of personal information by agencies and organisations, and direct an agency to conduct and provide me with a privacy impact assessment.[1] Since 12 March 2014 I also have enhanced enforcement powers such as the ability to make a determination where I initiate an investigation and to seek enforcement in the Federal Court.

Other privacy considerations

In addition to personal information privacy, the Bill also engages broader notions of privacy, including issues that go beyond data protection and extend to issues such as bodily privacy and surveillance. Examples of proposals that raise these issues include: the proposals to introduce a delayed notification search warrant scheme for terrorism offences and the proposals to extend the control order regime and preventative detention order (PDO) regime for a further ten years.

I note that the Statement considers whether these proposals are compatible with the right to protection against arbitrary and unlawful interferences with privacy in Article 17 of the ICCPR. As identified in the Statement, where the proposed measures impact upon the privacy interests of individuals, consideration should be given to whether those measures are proportionate and necessary; that is, whether they appropriately balance the intrusion on individuals' privacy with the need to protect the public from threats to national security (including terrorism).

To assist the Joint Committee in considering whether these measures are necessary and proportionate, the Joint Committee might wish to consider the approach contained in the OAIC's 4A Framework (a copy of the framework can be found in Appendix A). The 4A Framework outlines a four step approach for assessing and implementing new law enforcement and national security powers. 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 by asking:

1. Whether the proposed measure is a proportional response, in light of its impact on privacy and existing community expectations?

2. Under what circumstances the powers can be exercised?

---

[1] A privacy impact assessment is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, mitigating or eliminating that risk.

3. What safeguards are in place?

4. Whether there are any built in review mechanisms?

I also draw the Joint Committee's attention to the submission made by the then Office of the Privacy Commissioner to the Senate Legal and Constitutional Legislation Committee (the Senate Committee) in relation to the Inquiry into the provisions of the *Anti-Terrorism Bill (No. 2) 2005*, which introduced the control order and PDO regimes (a copy of the submission can be found in Appendix B).

Specific Comments

In light of the tight time-frame, I have given more detailed consideration to the proposed measures that involve the handling of personal information and that, therefore, may engage my regulatory responsibilities under the Privacy Act.

Listing the Attorney-General's Department as a 'designated agency' for the purpose of accessing AUSTRAC information

The Bill amends the definition of a 'designated agency' in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) to include AGD. This will enable AGD to access financial intelligence information held by AUSTRAC (AUSTRAC information), subject to written authorisation provided by the AUSTRAC CEO.

I appreciate that the intention of this amendment is to enable AGD to more efficiently and effectively develop policy to combat terrorism financing risks. However, I am concerned that the extension of the definition of a designated agency to include AGD represents a significant shift in the types of entities that are permitted to access AUSTRAC information; specifically, that designated agencies are primarily agencies that have law enforcement functions and activities, whereas AGD is seeking access to assist in its policy making activities.

In expressing this concern, I am mindful that there are a range of privacy safeguards that apply to the handling of AUSTRAC information. Importantly, I understand that when the AUSTRAC CEO is considering whether to give a designated agency access to AUSTRAC information, the CEO must have regard to privacy matters (see s 212 of the AML/CTF Act). Further, where AUSTRAC information includes personal information and that information is disclosed to a designated agency that is also an APP entity (such as AGD), the APPs regulate how that personal information must be handled by the designated agency. In particular, under APP 3.1, agencies requesting access to AUSTRAC's information will have to consider their obligation to only collect personal information that is reasonably necessary for, or directly related to, one or more of their functions or activities.

Additionally, I note that in considering the privacy impacts of this amendment the Statement of Compatibility with Human Rights suggests that the majority of AUSTRAC information accessed by AGD would be considered at an aggregated level. I advise that if the information is aggregated to a level where it is no longer about an identifiable individual or an individual who is reasonably identifiable (that is, where the information has been de-identified), the information is no longer personal information and is not regulated by the Privacy Act.

However, whilst it is always preferable from a privacy perspective to de-identify personal information before using or disclosing the information, I recognise that in some circumstances the purpose of the use or disclosure cannot be served by de-identification of information.

With those considerations in mind, I suggest that the Joint Committee seek further clarification about the nature of the information likely to be sought by AGD and whether any of that information would be sufficiently aggregated to make it de-identified. Further, that the Joint Committee consider whether AGD's collection of AUSTRAC information that is personal information (that is, information that is not sufficiently aggregated to ensure that it is de-identified) is reasonably necessary for, or directly related to, AGD's functions or activities.

Collection of biometric information by automated border clearance systems

I understand that the Bill amends the *Migration Act 1958* (the Migration Act) to allow an automated border clearance system (authorised system), such as a SmartGate, to collect certain personal information, including biometric information (for example, facial images).

I advise that since the reforms to the Privacy Act, which came into effect on 12 March 2014, this type of personal information is considered to be 'sensitive information' and, therefore, attracts a higher level of protection under the Privacy Act. Specifically, biometric information, such as a facial image, will be sensitive information where it is used for the purpose of automated biometric verification or biometric identification (for example, when it is used by a SmartGate).

APP 3 requires that sensitive information must only be collected with the consent of the individual unless one of the listed exceptions applies. Those exceptions include where the collection is authorised or required by law. While this means that if the Bill is passed an individual's consent will no longer be required for the collection of this type of biometric information, I note the assurance in the Statement that any handling of this information will be undertaken in accordance with the APPs. In particular, the Statement notes the steps that will be taken to ensure compliance with the notice obligations in APP 5 – namely, that individuals will be notified about the collection of this information through signs, information sheets, and information on DIBP's and Customs' websites. Further, the Statement makes clear that this biometric information will be subject to the existing restrictions in the Migration Act in relation to the purposes for which the information may be collected, used and disclosed.

In making these observations, I am mindful of the rapid growth in the use of biometric technology, and I am taking steps to ensure that agencies and organisations are aware of the addition protections that are afforded to this type of sensitive personal information by the Privacy Act.

In addition to the assurance that this information will be handled in accordance with the APPs, I understand that this type of biometric information (facial images) is currently being collected by the DIBP. However, I am mindful that the proposed amendment does allow for the making of regulations prescribing additional categories of biometric information (referred to in the Migration Act as personal identifiers), such as fingerprints and iris scans.

I appreciate the need to ensure that the law is able to accommodate changes in technology and, therefore, do not raise any concerns about this amendment. In saying this, I would, however, expect that any proposal to extend the types of biometric information prescribed in the regulations would be subject to appropriate public consultation. In addition, I would welcome any invitation to provide feedback on the likely privacy impacts of such a proposal.

Authorising DIBP to collect and retain personal information contained in a document

I understand that the Bill introduces a new provision into the Migration Act that authorises a clearance authority (including both an authorised system and an authorised border clearance officer) to collect and retain any information contained in a document that is presented by an individual to the clearance authority. Further, that this would include the clearance officer making a physical or electronic copy of any information contained on the document or, where the document is an electronic document, such as an ePassport, stored in the document.

I understand that the effect of this amendment is not to authorise the collection of any additional information by DIBP, as this information is already able to be collected from an individual by a border clearance officer. Rather, the amendment is intended to take account of developments in border security technologies (such as the introduction of SmartGates) and the shift towards an automated border clearance system.

Further, I note that the Migration Act currently contains provisions that will regulate how this information must be handled. As identified above, those safeguards are supplemented by certain obligations in the APPs, including those relating to notice (APP 5), quality (APP 10) and security (APP 11).

With these considerations in mind, I do not raise any concerns in relation to this amendment.

Advanced identification of persons leaving Australia

I understand that the Bill amends the Migration Act to extend airlines' obligation to provide Australian border authorities (DIBP and Customs) with information about inward bound passengers and crew, to include information about departing passengers and crew. The information that must currently be reported is personal information and includes the incoming passenger or crew members name, passport number, nationality and (in certain circumstances) their date-of-birth and sex.[2] I note that this amendment does not purport to expand the types of personal information collected, only to extend the reporting obligation to include travellers and crew that are departing Australia. Further, that the information collected is information that is already collected by the border authorities when the passenger or crew member presents at the border.

---

[2] The Department of Immigration and Boarder protection (DIBP, formally the Department of Immigration and Citizenship) (2008) *Australia's APP Advance Passenger Processing System: Check-in Guide*, Commonwealth of Australia, available online at: <http://www.immi.gov.au/managing-australias-borders/border-security/air/airlines/app-checkin.htm>.

I note that, as is clearly identified in the Statement, this information will need to be handled by DIBP and Customs in accordance with the APPs. Further, I acknowledge that in addition to security considerations, there are benefits to the individual, in terms of reduced border processing time, by DIBP and Customs collecting this information in advance of the passenger or crew member presenting at the border (at the time of check-in).

With these considerations in mind, I do not raise any concerns in relation to this amendment.

Should the Joint Committee require any further information please contact Este Darin-Cooper, Director of Privacy Law and Practice, on

Yours sincerely

Timothy Pilgrim
Australian Privacy Commissioner

3 October 2014

Australian Government
Office of the Australian Information Commissioner

Privacy fact sheet 3

4A framework – A tool for assessing and implementing new law enforcement and national security powers

July 2011

The Office of the Australian Information Commissioner has developed a proposed framework for assessing and implementing new law enforcement and national security powers. The 4A framework sets out a lifecycle approach from development to implementation and 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.

Analysis

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.

Authority

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.

Accountability

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.

Appraisal

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?

The information provided in this fact sheet is of a general nature. It is not a substitute for legal advice.

For further information
telephone: 1300 363 992
email: enquiries@oaic.gov.au
write: GPO Box 5218, Sydney NSW 2001
GPO Box 2999, Canberra ACT 2601
or visit our website at **www.oaic.gov.au**

Appendix B:

Australian Government

Office of the Privacy Commissioner

Submission by the Office of the Privacy Commissioner

to the Senate Legal and Constitutional Legislation Committee

Inquiry into the provisions of the Anti-Terrorism Bill (No. 2) 2005

November 2005

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner (the Office) is an independent statutory body responsible for promoting an Australian culture that respects privacy. The *Privacy Act 1988* (the Privacy Act) covers Australian and ACT Government agencies, businesses with an annual turnover of more than $3 million, the private health sector, small businesses that trade in personal information and credit providers and credit reporting agencies. The Privacy Commissioner has responsibilities under the Privacy Act and other federal legislation to regulate the way agencies and organisations collect, use, store and disclose individual's personal information.

Background and overview

2. In April 2002 and August 2004, the Office made submissions to the Senate Legal and Constitutional Committee Inquiries into, respectively, the *Security Legislation Amendment (Terrorism) Bill 2002* (and related Bills)[1] and the *Anti-Terrorism Bill (No.2) 2004*.[2]
3. The Office remains of the view, expressed in those submissions, that there should be an appropriate balance between the need for security and the right to privacy.
4. The right to privacy is not an absolute. It is often necessary to balance privacy with other important social interests, such as the safety and security of the community. This does not diminish the role played by privacy in democratic societies in according individuals the freedom to pursue their daily lives with appropriate respect, dignity and anonymity. Rather, the challenge is to how to achieve an appropriate balance.
5. The Office welcomes the Committee's Inquiry into the *Anti-Terrorism Bill (No.2) 2005* (the Bill) and hopes that this submission will assist the Committee in its consideration of the Bill. The Committee should note that the scope of the submission is limited to matters relevant to privacy issues.
6. The Office notes that a number of new provisions contained in the Bill will expand the power of law enforcement and intelligence agencies to collect personal information about individuals, including through routine surveillance and electronic tracking. Any such expansion is likely to diminish, to varying degrees, the privacy of individuals by reducing their ability to control personal information about themselves.
7. The Office has not commented on every proposed amendment in the Bill. However, as a general point, in relation to the creation of new offences, or the amendment of existing offences, for example; by changes to definitions of offences, law enforcement or intelligence

[1] OFPC *Submission to the Inquiry into the Terrorism Bills* April 2002 <available at http://www.privacy.gov.au/publications/secleg.pdf .
[2] OFPC *Submission to the Inquiry into the Provisions of the Anti-terrorism Bill (No.2) 2004* August 2004 <available at http://www.privacy.gov.au/publications/antitersub.pdf

.

agencies will be permitted to perform acts and practices that may otherwise, in the absence of that change, constitute an interference with an individual's privacy. Such changes as proposed in the Bill should be proportional to the need for greater security.

8. As one means of making judgements between competing priorities, such as privacy and security, the Office has developed and refined a framework by which new legislative measures could be assessed (see Attachment 1).

9. This framework is underpinned by the recognition that measures that diminish privacy should only be undertaken where they are necessary and proportional to address the immediate need, and are subject to appropriate and ongoing accountability measures and review. The Office commends the framework to the Committee when it is considering the Bill.

10. The Office also notes that some aspects of the Bill, specifically Schedules 8 and 9, would benefit from a formal Privacy Impact Assessment (PIA). Such an assessment process has particular value where an initiative involves the following:

    - the handling of personal information in large quantities and its aggregation into large databases
    - the personal information involved is sensitive information, such as financial information and
    - the initiative is significant, for example; in its size, complexity or scope.

11. It is likely that a PIA would clarify the need and inform the development of these schedules of the Bill, and assist any subsequent implementation of them.

Application of the Privacy Act to the Bill

12. The Privacy Act sets out 11 Information Privacy Principles (IPPs) that govern the way Australian Government agencies (and their outsourced providers) collect, use, disclose and handle personal information. The principles also give individuals the right to gain access to information held about them and they oblige agencies to correct information if it is inaccurate. In a similar way, many private sector organisations are governed by the National Privacy Principles (NPPs) as set out in Schedule 3 of the Privacy Act.

13. There are exceptions under both the IPPs and the NPPs that allow agencies or organisations to use or disclose personal information when it is 'required or authorised by or under law'. These exceptions may lessen the protection of an individual's personal information that would have otherwise been provided by the Privacy Act.

14. While it is accepted that there is a need for governments to combat threats to national security such as terrorism, they should also be

concerned to ensure that individuals' personal information, most particularly in the case of persons about whom there is no cause for suspicion, is only collected, used and disclosed, when this is clearly necessary.

Provision for review of the amendments introduced by the Bill

15. Clause 4 of the Bill states the Council of Australian Governments (COAG) agreed on 27 September 2005 that Schedules 1, 3, 4 and 5 be reviewed after 5 years, together with certain unspecified state law.

16. The Office supports the intent of this clause. However, it is the Office's view that given the amendments made by this Bill in relation to privacy issues, it is desirable that a transparent review of these amendments be conducted at a specified time. The current drafting of clause 4 does not appear to impose a clear statutory obligation on any party to initiate and conduct such a review.

17. Further, the office suggests there are several Schedules that may impact on the way personal information is collected and handled and would benefit from review for oversight reasons and/or to maintain consistency with other legislative developments. These are:

- Schedule 6, which affords increased powers to the Australian Federal Police to demand documents without judicial oversight, including in contexts unrelated to terrorism
- Schedule 8, on optical surveillance in airports which may be affected by the development of proposed national guidelines on the use of CCTV and
- Schedule 9, on financial transaction reporting, which may be affected by ongoing reform in Anti-Money Laundering (AML) regulation.

18. In considering a suitable mechanism for review the Office suggests as a model section 4 of the *Security Legislation Amendment (Terrorism) Act 2002*.

Schedule 4—Control orders and preventative detention orders

19. Schedule 4 introduces new powers to issue control and preventative detention orders for the purpose of protecting the public from terrorist acts. The exercise of these powers is likely to result in law enforcement and intelligence agencies collecting and using greater quantities of personal information. Those powers need to be well considered to ensure an

appropriate balance is achieved between community safety and individual privacy.

Handling of personal information collected under control and preventative detention orders and other activities

20. Changes in information handling include new section 104.5(3)(j), which may require an individual to be photographed as part of a control order, and new section 104.5(3)(k), which makes it a requirement that impressions of fingerprints are taken. This information is to be collected as part of a control order and can be invoked without charge.

21. The Office notes that new section 104.22(1) requires that the fingerprints and photographs collected under the above sections, must only be used for the purpose of "ensuring compliance with the relevant control order". This requirement seems consistent with the privacy principle that information only be used or disclosed for the purpose for which it was initially collected.

22. New section 104.22 outlines a retention period for fingerprints and photographs taken under new section 104.5(3). This section requires that once a 12 month period has elapsed following the cessation of a control order and provided no proceedings have been brought or they have been discontinued, the information is to be destroyed as soon as practicable. While the Office supports the destruction of records when they are no longer required and the inclusion of a set period is useful, it is not made clear in the Bill or the Explanatory Memorandum why the retention period has been prescribed as 12 months.

23. Similarly, it is not clear why the retention period (under new section 105.44) for information collected under new section 105.43 (pursuant to a preventative detention order) has been prescribed as 12 months

24. The Office would suggest that the Committee may wish to consider whether different retention periods may be more appropriate, for example; a lesser period of 6 months may be appropriate in some circumstances.

25. The Office notes that new section 104.5(3)(d) specifies that a term of an interim control order may be to wear a tracking device, section 105.23 gives a power to conduct a frisk search and section 105.24 an ordinary search. Whilst these types of activity may not ordinarily be regulated by the Privacy Act, records created from such activity may be.

26. Given that personal information may therefore be collected through these new methods it is important to balance the privacy protections with the potential collection and use of the information. However, unlike elsewhere in the Bill, these sections do not address the question of how long personal information, once collected in these ways, may be retained. An approach, which is consistent with best privacy practice, would be to destroy the information once it is no longer necessary for the purpose for which it was collected.

27. The Office acknowledges that some of the information collected through these activities will not always fall within the definition of personal information provided in section 6 of the Privacy Act, and therefore may not be regulated by the IPPs or NPPs. The handling of such information, and the activities themselves may, however, fall within the broader notion of privacy (which includes bodily privacy) covered by Article 17 of the International Covenant on Civil and Political Rights.[3]

Reporting of control and preventative detention orders

28. New sections 104.29 and 105.47 require the Attorney-General to report to Parliament annually on the operation of control orders and preventative detention orders respectively for the previous year. The Office supports the requirements for the Attorney-General to report to the Parliament regularly.

Schedule 6—Powers to obtain information and documents

General Comments

29. The Office notes that Schedule 6 of the Bill appears to represent an expansion in the information collection powers of the Australian Federal Police (AFP). These include new sections 3ZQM, 3ZQN and 3ZQO which are discussed in greater detail below.

30. The result of this Bill being enacted would be to permit greater collection of personal information by the AFP including from private sector organisations, without warrant. While such collection and disclosure would comply with the AFP's obligations under the Privacy Act, as it would be authorised by law, careful consideration should be given to the enactment of such powers as they may detract from the intent and spirit of the Privacy Act.

31. An agency's collection of personal information must comply with the Information Privacy Principles (IPPs), which are underpinned by the expectation that the handling of personal information will be open and transparent and in a way that the individual concerned would reasonably expect. The IPPs expressly require that, amongst other things, the collection of personal information should be necessary for a lawful purpose or for a purpose directly related to that purpose.[4] In addition, the collector must take reasonable steps to ensure collection does not intrude to an unreasonable extent upon the personal affairs of the individual concerned.[5] Where personal information is collected directly from the

[3] http://www.unhchr.ch/html/menu3/b/a_ccpr.htm
[4] IPP 1.1
[5] IPP 1.3

individual, the individual should be provided notice of the collection, including what the information may be used for.[6]

32. In expanding the powers of law enforcement agencies, this Schedule invests a significant degree of unilateral authority in law enforcement officers going about their required duties with no corresponding guidance as to how this authority should be exercised. Specifically, the test required to request documents is: the authorised AFP officer "believes on reasonable grounds" and the officer must determine what is "relevant to". There is no obvious guidance on how these subjective terms should be interpreted, posing the risk that they may be interpreted broadly. The Office suggests that such powers should be accompanied by guidance as to how they should be executed.

Power to request information or documents about terrorist acts from operators of aircraft or ships (new section 3ZQM)

33. Under this provision, there is the potential for a large quantity of information to be collected from aircraft operators and operators of cruise liners. As a result, the personal information of large numbers of individuals who are not the subject of investigations and about whom there is no cause for suspicion, could be collected. Such an outcome sits uncomfortably with the notion of necessary collection. It would be preferable for there to be greater explanation as to how such routine surveillance would be useful, including whether it is a necessary and proportional response to the need for greater security.

34. As with the provisions relating to bodily searches and tracking devices, this section does not address the question of how long personal information, once collected, may be retained. As previously noted, an approach which is consistent with best privacy practice would be to destroy the information once it is no longer necessary for the purpose for which it was collected, particularly in relation to the information of people who may not be the subject of interest to law enforcement authorities.

Power to obtain documents relating to serious terrorism offences (new section 3ZQN)

35. New section 3ZQN authorises the collection of documents relevant to serious terrorism offences which "relate to" the matters outlined in new section 3ZQP. While the types of personal information that may be collected under this section are specified, the Office notes that they are prescribed broadly. In addition, it is noted that information may be required where that information 'relates to' the prescribed matters.

36. This would seem to create a power for the AFP to demand personal information without judicial warrant that is considerably wider than the power which currently exists. This section appears to substitute the use of notices in place of obtaining warrants. It is the Office's understanding

[6] IPP 2

that only the latter are subject to judicial oversight. The need for this additional power without judicial oversight is not readily apparent.

37. In the absence of further information the Office suggests that a warrant issued by a judicial officer would provide a more appropriate level of oversight.

38. It should be noted that any collection made under this new section, while permitted, would still result in the AFP having obligations under the IPPs as to how personal information may be handled subsequent to collection.

Power to obtain documents relating to serious offences (new section 3ZQO)

39. New section 3ZQO provides for a notice to be issued to a person to produce documents in relation to a 'serious offence'. A 'serious offence' is defined in the Crimes Act and does not include terrorism offences.

40. The accompanying Explanatory Memorandum states that this Bill "...improves the existing strong federal regime of offences and powers targeting terrorist acts and terrorist organisations. The Bill is the result of a comprehensive review of existing federal legislation that criminalises terrorist activity and confers powers on law enforcement and intelligence agencies to effectively prevent and investigate terrorism".[7]

41. Discussion around the Bill has, in turn, focused on the extent to which the new powers are necessary and proportional as measures to combat the risks posed by terrorism. The introduction of measures that expand the powers of law enforcement agencies to investigate other offences seems to fall outside of the stated purpose of the Bill. Such measures are likely to have policy objectives distinct from those that underpin the main provisions of the Bill relating to terrorist activity and should be able to be separately scrutinised and pursued through stand-alone legislation.

42. The Office notes that this new section covering serious (non-terrorism) offences includes an element of external oversight, in that a notice issued under the section must be subject to an application made to a Federal Magistrate. Such oversight is not provided in case of serious terrorism offences under new section 3ZQN (as discussed at paragraphs 35-38). .

43. The Office recommends that the provisions of new section 3ZQO be pursued through separate legislation after appropriate scrutiny and consultation.

[7] Explanatory Memorandum to the Bill, p.1.

Schedule 8—Optical surveillance

44. The Explanatory Memorandum to the Bill explains that Schedule 8 will insert a new Division into the *Aviation Transport Security Act* (2000) (ATS Act) by enabling the Minister to determine a code regulating and authorising the use of optical surveillance devices at airports. This code would operate to the exclusion of state or territory law.

45. The use of closed circuit television is expected to assist in the provision of aviation security.[8] However, it is noted that new section 74J explains that the purpose of the proposed division includes preventing and detecting breaches of the ATS Act or *any other law of the Commonwealth*. Such a provision seems to envisage optical surveillance being used for purposes that may be unrelated to either airport security or anti-terrorism.

46. The Office acknowledges that the use of surveillance devices may assist with airport security and anti-terrorism. This potential was noted, for example, in the report of the recent *Airport Security and Policing Review*.[9]

47. However, it should also be recognised that such technology allows for the routine and indiscriminate surveillance of large numbers of people, for example, in public spaces such as airport arrival halls. For many of these people, there may be no cause for suspicion and hence no reason to collect information about them.

48. One of the primary principles of privacy is that personal information should only be collected where it is necessary. Accordingly, it is important that proposals envisaging routine optical surveillance are pursued carefully so as to ensure an appropriate balance is struck between the public interest in a safe and secure society and the right of individuals to privacy.

49. Achieving such a balance requires that optical surveillance measures should only be pursued where necessary to achieve a clear objective and where such measures constitute a proportional response to a defined threat or problem. Such measures should also be subject to appropriate oversight to ensure that personal information is not misused.

Optical surveillance code for aviation industry participants

50. The Office notes that a code made under this Schedule would apply to 'aviation industry participants', including private sector organisations such as airlines and airport operators, as well as other organisations prescribed by regulation. In many cases, such organisations will fall under the jurisdiction of the Privacy Act and be bound by the National

[8] Explanatory Memorandum to the Bill, p.95.
[9] Australian Government "An independent review of airport security and policy for the Government of Australia" conducted by The Rt Hon Sir John Wheeler DL September 2005 <available at http://www.aspr.gov.au/docs/Security_and_Policing_Review_PUBLIC.pdf

Privacy Principles in the manner they handle personal information. Similarly, aviation industry participants that are Australian Government agencies will be bound by the Information Privacy Principles. Other entities, particularly some small businesses or state or territory government bodies, would not fall under the jurisdiction of the Privacy Act.

51. Although neither the Bill or the Explanatory Memorandum explain the purpose of the code, the Office notes that new section 74K(2) states that the code "...may regulate and authorise the use or disclosure of a signal, image or other information obtained by the use of the optical surveillance device". Such a provision seems to provide an opportunity for appropriate regulation to be made to limit the way in which personal information collected by CCTV may be handled. The Office notes that such regulation, particularly if made consistent with the principles of the Privacy Act (including provision for complaint handling and oversight, such as independent audit), could help engender community confidence that personal information collected by optical surveillance to prevent and investigate terrorism will not be misused.

52. Making such proposed codes consistent with the principles of the Privacy Act would also ensure that organisations not currently under the Privacy Act's jurisdiction, for example, companies with a turnover of less than $3 million, handle information collected pursuant to the code in an appropriate way.

53. The Office suggests that the section provide for the Minister to consult with various parties when making such a code, including with the Privacy Commissioner. Additionally, the section should specify the need for and manner of any future review of the code.

Proposed National Code of Practice for CCTV for the mass passenger transport sector

54. The Office also notes that the Council of Australian Governments (COAG) has agreed to the development of a National Code of Practice for CCTV systems for the mass passenger transport sector, which will contain guidelines on the handling and privacy of personal information.[10] The relationship between this COAG initiative and Schedule 8 of the Bill is unclear.

55. As noted in paragraph 10, the development of an optical surveillance code for the purposes of this Schedule could be usefully informed by conducting a Privacy Impact Assessment as part of its development.

[10] Council of Australian Governments (COAG) "Communiqué: Special Meeting On Counter-Terrorism" 27 September 2005 <available at http://www.coag.gov.au/meetings/270905/coag270905.pdf>

Schedule 9—Financial transaction reporting

56. The Explanatory Memorandum to the Bill notes that Schedule 9 contains amendments to the *Financial Transaction Reports Act 1988* (FTR Act) to "...better implement the Financial Action Task Force on Money Laundering's (FATF's) Special Recommendations VI (SR VI), VII (SR VII) and IX (SR IX)". These amendments are summarised below in terms of the Special Recommendations.

Registration of informal networks

57. To implement SR VI, Items 5 and 11 of the Schedule will require the registration of 'informal networks' for the transmission of money or value. The term 'informal networks' is broadly canvassed in the Explanatory Memorandum. It is understood, however, that certain cash dealers will be required to provide to AUSTRAC 'prescribed particulars' regarding identifying information. The scope of these amendments is unclear and it is difficult to determine how much more personal data will be collected and stored by AUSTRAC.

International wire transfers to include customer data

58. To implement SR VII, Item 10 of the Schedule will require cash dealers to include identifying particulars regarding their customers in international funds transfer instructions. These instructions, whether into or out of Australia, are currently reported to AUSTRAC under the FTR Act. Again, there is no indication of the scope of these amendments and no understanding of the volume of personal information collected by AUSTRAC.

Interdiction of cash couriers

59. To implement SR IX, a number of items including Item 9, will require a transborder courier, of both currency and 'bearer negotiable instruments', to prepare, on request, a report to AUSTRAC of details about the courier and/or the person on whose behalf the instruments or currency is being carried. These obligations are supported by powers under Item 18 to question and search couriers in certain circumstances.

60. As a general observation, some amendments, intended to extend the scope of the reporting obligations and the provision of personal information to AUSTRAC, are supported by criminal sanctions, including terms of imprisonment (see, for example, Items 12, 13, 14 and 15).

Existing Anti-Money Laundering (AML) reform

61. Since 2003, the Office has been consulted by the Attorney-General's Department (AGD) on privacy issues relevant to the proposed Anti-Money Laundering Bill (the proposed AML Bill). It is understood that the provisions of proposed AML Bill were intended to implement all

FATF Recommendations, including the Special Recommendations, to meet the challenges of money laundering and terrorist financing.

62. The Office understands that the AML Bill was being developed through a carefully planned process of public consultation, including the conduct of 'roundtable' discussions between the Minister and industry leaders. An Exposure Draft is to be released before the end of the year.[11] Widespread consultation on this legislation with the community has been, and continues to be, supported by the Office.

63. In advice to the AGD, the Office has previously advocated the strong desirability of conducting a Privacy Impact Assessment (PIA). As noted in paragraph10 of this submission proposed Schedule 9 has the attributes that support the adoption of a PIA process.

National privacy protections for financial data and the importance of community confidence

64. As the amendments in Schedule 9 are understood, there will be new reporting obligations placed on a comparatively large number of financial entities. In terms of the Privacy Act, some of these entities may be exempt from the legislative obligations usually attaching to the information handling acts and practices of private sector organisations.[12] It is also unclear whether the current amendments are intended to cover the agencies of the states and territories, only some of which are subject to privacy legislation.

65. The implications of this uneven coverage of the private sector and, possibly, many public sector agencies, is that large amounts of often sensitive financial and other personal data handled by these entities will not be protected by any privacy legislation - national, state or territory. This situation is compounded by the current obligations in Part VIA of the FTR Act for financial institutions to retain data, such as customer-generated financial transaction documents, for a minimum of seven years.

66. Community research conducted by the Office has demonstrated a notable reluctance in the community to deal with business, when there are concerns about the privacy of their personal information being protected.[13] The existence of, and compliance with, effective privacy regulation enable business to enlist community confidence. The effective implementation of legislative measures to counter money-

[11] "Government strengthening anti-money laundering and counter-terrorist financing", Senator The Hon Chris Ellison, Minister for Justice and Customs (Media Release) 11 October 2005. Available at http://www.ag.gov.au/agd/WWW/justiceministerHome.nsf/AllDocs/2CF4C32CCDD05F5CCA25709700290D9E?OpenDocument [9 November 2005].

[12] See, generally Part II of the *Privacy Act 1988 (Cth)*. Available at: http://www.privacy.gov.au/publications/privacy88_030504.doc.

[13] Office of the Privacy Commissioner *Privacy and the Community* (July 2001). Available at http://www.privacy.gov.au/publications/rcommunity.html#4.2.

laundering and the financing of terrorist activities will depend in large part on the willing cooperation of the business community in providing critical financial data to law enforcement agencies. This in turn will be underpinned by the understanding and confidence on the part of the community as to what happens to their financial data.

67. The Office is concerned about the consequences of bringing forward the amendments to the FTR Act before the planned consultation process for the proposed AML Bill. Such an outcome may produce an unintended loss of community and business confidence in the anti-money laundering and counter-terrorist financing framework .

68. Rather than the amendments to the FTR Act being made *at this time,* the Office recommends that Schedule 9 remain the subject of the careful consultation and assessment process being undertaken by the Minister for Justice and Customs and his Department as part of the AML reform agenda.

Schedule 10—ASIO powers etc

69. While the acts and practices of ASIO do not fall within the jurisdiction of the Privacy Act, the Office would still recommend that any expansion in its powers in relation to the collection, use and handling of personal information should be accompanied by strong guidance in relation to best practice in the handing and disposal of that information.

70. The new section 23 introduced by Item 2 of Schedule 10 grants ASIO additional powers to collect personal information from the operators of ships and aircraft, including regarding crew and passengers. The Schedule introduces an offence for not producing such documents. In many cases, the exercise of this power could result in the collection of personal information about individuals who are not the subject of inquiry and about whom there is no cause for suspicion.

71. The Office notes that there is no guidance on the grounds on which the Director-General, or senior officer authorised in writing, may authorise an ASIO officer to exercise this power (see, new section 23(6)).

72. The Office suggests that guidance from the Inspector-General of Intelligence and Security in relation to the collection, use and disposals of records by ASIO, particularly those relating to individuals not the subject of interest to ASIO would be beneficial.

Summary

73. The Office of the Privacy Commissioner (the Office) is of the view that there should be an appropriate balance between the need for security and the right to privacy.

74. The right to privacy is not an absolute. It may be necessary to balance this right with other important social interests, such as the safety and security of the community.

75. This Office notes that a number of new provisions contained in the Bill will expand the power of law enforcement and intelligence agencies to collect personal information about individuals, including through routine surveillance and electronic tracking. Any such expansion is likely to diminish, to varying degrees, the privacy of individuals by eroding their ability to control personal information about themselves. Such expansions lessen the protection of an individual's personal information that would have otherwise been provided by the Privacy Act.

76. The Office notes that a formal Privacy Impact Assessment could assist in clarifying the need for, and subsequently implementation of several aspects of the Bill where large amounts of personal information will be collected, notably Schedules 8 and 9. (see paragraphs 10 and 11, paragraph 55 on Schedule 8 and paragraph 63 on Schedule 9).

77. The Office notes the importance of reviewing the operation of the changes and recommends that explicit statutory commitment be given to their review, together with detailed process for the review (see paragraphs 15-18).

78. The Office has not commented specifically on changes to definitions in relation to criminal offences, including those introduced in Schedules 1, 3 and 7. In general though, the creation of new offences, or the amendment of existing offences, will often permit law enforcement or intelligence agencies to perform acts and practices that may otherwise, in the absence of that law, constitute an interference with an individual's privacy. Accordingly, any such changes to law should include as a consideration whether privacy rights will be diminished, the impact on individuals should this occur and whether such an outcome is, on balance, proportionate to the need for greater security.

79. Schedule 4 outlines the retention periods for fingerprints and photographs taken pursuant to new sections 104.5(3) and 105.43. It is not made clear in the Bill or the Explanatory Memorandum why this information needs to be retained for 12 months after a control or preventative detention order ceases and where there is no ongoing action being taken against the individual. The Office would suggest that the Committee may wish to consider whether different retention periods may be more appropriate, for example; a lesser period of 6 months may be appropriate in some circumstances.(see paragraphs 20-24).

80. The Office also notes controls should be included in the Bill in relation to the collection of personal information from the use of tracking devices and searches outlined in Schedule 4. (see paragraphs 25-27)

81. The Office recommends that the provisions introduced by Schedule 6 (new section 3ZQO) concerning offences that are not terrorism offences be pursued through separate legislation after appropriate scrutiny and consultation. (see paragraphs 39-43).

82. As regards the provisions introduced by Schedule 8, the Office notes that the use or optical surveillance, such as closed circuit television (CCTV), poses the risk of unnecessary routine and indiscriminate surveillance of large numbers of people, about who there may be no cause for suspicion. (see paragraphs 44-49)

83. The Office notes that the provision in Schedule 8 for the Minister to issue a statutory code of practice as to how information collected through optical surveillance may be handled. The Office notes that such regulation, particularly if made consistent with the principles of the Privacy Act (including provision for complaint handling and oversight, such as independent audit), could help engender community confidence that personal information collected by optical surveillance, to prevent and investigate terrorism, will not be misused. (see paragraphs 50-53)

84. The Office suggests that Schedule 8 provide for the Minister to consult with various parties when making a code for optical surveillance, including with the Privacy Commissioner and that a Privacy Impact Assessment could usefully inform the code's development. (see paragraph 53 and 55).

85. In relation to the amendments to the *Financial Transactions Reports Act (1988)* (FTR Act) contained in Schedule 9, the Office notes the valuable widespread consultation that has been conducted by the Minister for Justice and Customs and his Department on reform of Anti-Money Laundering and the Suppression of Terrorism Financing regulation since 2003. (see paragraphs 56-63)

86. Rather than the amendments to the FTR Act being made at this time, the Office recommends that Schedule 9 remain the subject of the careful consultation and assessment process being undertaken as part of the AML reform agenda. (see paragraphs 67-68)

87. The Office suggests that guidance from the Inspector-General of Intelligence and Security in relation to the collection, use and disposals of records by ASIO, particularly those relating to individuals not the subject of interest to ASIO would be beneficial. (see paragraphs 69-72)

Attachment 1

Office of the Privacy Commissioner

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

The Office of the Federal Privacy Commissioner has developed a proposed framework for assessing and implementing new law enforcement and national security powers. The framework sets out a life cycle approach to such proposals from development to implementation and 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?