Australian Government
Office of the Australian Information Commissioner

Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010:

Submission to Senate Legal and Constitutional Affairs Legislation Committee

November, 2010

Key recommendations

The Office of the Australian Information Commissioner (the Office) appreciates the opportunity to provide a submission to the Senate Legal and Constitutional Affairs Committee on the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010 (the Bill).

The Office's main suggestions for improving and enhancing the privacy protections in the Bill are:

1. Using the former Office of the Privacy Commissioner's (OPC) 4A framework to assist in ensuring the proposed amendments contained in the Bill only apply in circumstances where it is necessary and proportionate to facilitate information sharing between intelligence and law enforcement agencies undertaking their legitimate functions.

2. Amending Item 5 in Schedule 1 of the Bill to explicitly reflect the stated policy intention of enabling the Australian Security Intelligence Organisation (ASIO) to provide technical assistance to law enforcement agencies in relation to telecommunications interception warrants issued to those agencies. To address potential gaps in privacy coverage, the Office suggests guidelines for law enforcement agencies on personal information handling practices are further developed with the assistance of the Office. It may also be appropriate for the guidelines issued by the Attorney General under section 8A of *Australian Security and Intelligence Organisation Act 1979 (Cth)* (ASIO Act) to be reviewed. The Office would be available to assist in any review process.

3. Further enhancing the privacy safeguards contained in Schedule 3 of the Bill relating to the disclosure of telecommunications data relating to missing persons by:

    - Introducing a set of binding rules or regulations to apply to the handling of telecommunications data related to missing persons.

    - Using consistent terminology to that used in Australian Privacy Principle (APP) 6 (2) (g).

    - Providing more detailed guidance on issues surrounding consent, such as determining capacity and establishing whether implied consent was obtained, in the Explanatory Memorandum to the Bill and in any binding rules or guidelines that are developed.

    - Inserting the word 'serious' before the word 'threat' in the proposed new section 182(2A)(b)(ii) of the *Telecommunications (Interception and Access) Act 1979 (Cth)* (TIA Act).

    - Including in Schedule 3 of the Bill a statutory review mechanism for the missing person provisions.

4. Developing guidance to assist law enforcement agencies to determine when a person is unable to consent or when it may be impracticable to gain the consent under the proposed amendments in Schedule 4. The Office also suggests the Explanatory Memorandum to the Bill expressly canvass where privacy issues may arise within the context of these proposed amendments to assist the issuing authority when considering the factors set out in section 116(2) of the TIA Act.

5. Establishing a privacy framework to support the information sharing arrangements set out in Schedule 6 of the Bill. This framework could be established through the development of a memorandum of understanding between participating agencies. The framework could include personal information handling guidelines covering the collection, use, disclosure, accuracy, complaint handling, storage, security, retention and destruction of personal information that falls within the scope of the information sharing arrangements**.**

6. The inclusion in Schedule 6 of the Bill of a statutory review mechanism that would allow the operation of the information sharing arrangements to be reviewed and assessed after a period of time.

Office of the Australian Information Commissioner

1. The Office of the Australian Information Commissioner (the Office) is established by the *Australian Information Commissioner Act 2010 (Cth)* (Australian Information Commissioner Act) and commenced operation on 1 November 2010. The Office is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two statutory office holders, the Freedom of Information Commissioner and the Privacy Commissioner. (The former Office of the Privacy Commissioner (OPC) became part of the Office on 1 November 2010).

2. The Office has three broad functions:

   - the privacy functions which are the functions set out in section 9 of the Australian Information Commissioner Act

   - the freedom of information (FOI) functions which are the functions set out in section 8 of the Australian Information Commissioner Act

   - the Information Commissioner functions which are the functions set out in section 7 of the of the Australian Information Commissioner Act.

Background

3. The Office appreciates the opportunity to provide a submission to the Senate Legal and Constitutional Affairs Legislation Committee on the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010 (the Bill).[1] The Office understands the main purpose of the Bill is to enable greater cooperation, assistance and information sharing within Australia's law enforcement and national security communities.[2] It is intended the Bill will achieve this by amending the *Telecommunications (Interception and Access) Act 1979* (TIA Act), the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the *Intelligence Services Act 2001* (IS Act).

[1] The Bill can be accessed at: http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbillhome%2Fr4456%22.

[2] Page 1 of the Explanatory Memorandum of the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010.

4. The Office recognises that there needs to be an appropriate balance between the public interest in law enforcement and national security agencies sharing information to facilitate their legitimate activities and the public interest in protecting the personal information of individuals. By implementing high standards of personal information handling law enforcement and national security agencies can help maintain information quality and assist in maintaining the integrity of investigations and inquiries. This will deliver better outcomes as well as promote community trust and confidence in the sharing of personal information by law enforcement and national security agencies.

The 4A framework

5. The right to privacy is not absolute and it is often necessary to balance this right with other important public interests, such as the public interest in maintaining the safety and security of the Australian community including preventing criminal activity or activity that puts Australia's national security at risk. As one means of making judgements between these priorities, the former OPC developed and refined a tool called the '4A framework' (see **Attachment A**).

6. The 4A framework is intended to assist government agencies consider personal information handling issues in their legislative measures specifically relating to new law enforcement or national security powers. It is underpinned by the recognition that measures that diminish privacy should only be undertaken where these measures are:

    - necessary and proportional to address the immediate need, and
    - subject to appropriate and ongoing accountability measures and review.

7. The Office believes consideration of the issues identified in the 4A framework will help in ensuring the proposed amendments contained in the Bill only apply in circumstances where it is necessary and proportionate to facilitate information sharing between intelligence and law enforcement agencies undertaking their legitimate functions. It will also ensure there are adequate privacy protections in place, including appropriate accountability and review mechanisms, for the collection, use and disclosure of personal information in the course of investigations and inquiries where law enforcement and national security agencies share personal information. These measures are likely to be important in promoting community confidence and trust in the proposed amendments contained in the Bill.

Privacy Act Coverage

8. The application of the Privacy Act 1988 (Cth) (Privacy Act) to those Australian intelligence agencies, Australian Government law enforcement agencies and State law enforcement agencies covered by the proposals in the Bill varies, thereby leading to potential gaps in privacy protection. The Information Privacy Principles (IPPs) in section 14 of the Privacy Act regulate the personal information handling practices of Australian Government and ACT agencies including those with enforcement and regulatory functions.

9. The Privacy Act does not extend to State or Territory authorities. The extent to which State authorities, including State law enforcement agencies, can provide adequate privacy safeguards will differ depending upon the level of privacy protection operating in the relevant jurisdiction.

10. The acts and practices of Australia's intelligence agencies – the Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Office of National Assessments (ONA), the Defence Intelligence Organisation (DIO), the Defence Imagery and Geospatial Organisation (DIGO) and the Defence Signals Directorate (DSD) are exempt from the Privacy Act.[3] The Australian Crime Commission (ACC) is similarly exempt.[4] Accordingly, any personal information collected, used or disclosed by these agencies when fulfilling their functions is not covered by 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.[5] In addition, an act or practice so far as it involves the disclosure of personal information to ASIO, ASIS or the DSD is exempt from the Privacy Act.[6]

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

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

[5] See section 7(1)(f) of the Privacy Act.

[6] See section 7(1A) of the Privacy Act.

11. The Office notes that although the intelligence agencies referred to above are not subject to the Privacy Act there are mechanisms in their enabling legislation which provide privacy protections. For example, section 15 of the IS Act requires the Ministers responsible for ASIS, DSD, and DIGO to make rules to regulate the communication and retention by the relevant agency of intelligence information concerning Australian persons. In making these rules the Minister is required to have regard to the need to ensure that the privacy of Australian persons is preserved as far as is consistent with the proper performance by the agency of its functions.[7]

12. Section 8A of the ASIO Act also provides for the Attorney-General to issue guidelines in relation to ASIO's function of obtaining, correlating, evaluating and communicating intelligence relevant to security. The guidelines include a section on the handling of personal information.

13. ACC officials and staff under section 51 of the *Australian Crimes Commission Act 2002 (Cth)* are prohibited from recording, communicating or divulging any information acquired by reason, or in the course, of the performance of their duties under this Act.

14. The Australian Law Reform Commission (ALRC) in its Report 108: *For Your Information: Australian Privacy Law and Practice* (ALRC Report)[8] recognised the activities of the ACC can have a significant impact on the privacy of individuals and there was a need to ensure personal information handled by the ACC was adequately protected. The ALRC recommended that the ACC, in consultation with the OPC, should develop and publish information-handling guidelines for the ACC and the Board of the ACC.[9] The information-handling guidelines should address the conditions to be imposed on the recipients of personal information disclosed by the ACC in relation to the further handling of that information.

[7] The DIO and ONA are not required under legislation to have similar rules regarding the communication and retention of intelligence information. However, following an administrative review of the IS Act in 2004, the Australian Government accepted a recommendation for these agencies to develop privacy guidelines in consultation with the Attorney-General and the Inspector-General of Intelligence and Security. These guidelines are consistent with the rules under section 15 of the IS Act.

[8] http://www.austlii.edu.au/au/other/alrc/publications/reports/108/.

[9] ALRC Recommendation 37-1. The ALRC also recommended that the Parliamentary Joint Committee on the ACC should monitor compliance of these information handling guidelines.

Exercise of warrant powers

15. The Explanatory Memorandum to the Bill sets out that Schedule 1 amends the TIA Act to enable ASIO to provide technical assistance to law enforcement agencies in relation to telecommunications interception warrants issued to those agencies.[10] However, Item 5 in Schedule 1 proposes to expand the persons who can be authorised under section 55 of the TIA Act to exercise a warrant to include officers or employees of ASIO and persons assisting ASIO in the performance of its functions. It does not contain any qualification that would limit this authorisation to the provision of technical assistance.[11] The Office suggests Item 5 in Schedule 1 of the Bill be amended to explicitly reflect the stated policy intention of the proposed amendments.

16. The Office supports the amendments in Schedule 1 that seek to limit the use and disclosure of information intercepted by ASIO on behalf of another agency.[12] The Office also supports the reporting requirements in the TIA being extended to include interception warrants conducted by ASIO on behalf of other enforcement agencies.[13]

17. The Privacy Act's coverage is limited as discussed at paragraphs 8, 9 and 10 above. For this reason, the handling of personal information obtained through an interception warrant may not always be subject to the Privacy Act. To address potential gaps in privacy coverage, the Office suggests guidelines on personal information handling practices be developed to ensure there is consistency in the way this type of information is handled by ASIO and law enforcement agencies. These guidelines could cover issues such as the accuracy, storage, security, retention and destruction of personal information and be developed with the assistance of the Office.

18. Guidelines issued by the Attorney General under section 8A of the ASIO Act currently provide ASIO with guidance on personal information handling practices. The current guidelines were issued on 12 October 2007 by the then Attorney-General, the Hon Philip Ruddock MP. Given the proposed expansion of ASIO's functions and powers under the Bill, the Office considers it may be appropriate for these guidelines to be to be reviewed. The Office would be available to assist in any review process.

[10] Page 4 of the Explanatory Memorandum of the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010.

[11] The clauses in the Bill refer to the Organisation. ASIO is defined in section 5 of the TIA Act as 'the Organisation'.

[12] Items 18, 19, 22 in Schedule 1 of the Bill.

[13] Items 23-26 in Schedule 1 of the Bill.

19. The Office notes the ALRC in its report recommended consistent privacy rules and guidelines be developed for intelligence agencies.[14] The Australian Government has announced it will consider this particular ALRC recommendation in its second stage response to the ALRC Report.

Disclosure of telecommunications data relating to missing persons

20. The Office empathises with the anguish faced by family and friends when someone they know cannot be located. However, the Office also recognises that competent adults in our society have the freedom to decide to lead their lives as they choose within the boundaries of the law. Individuals who have chosen to disassociate themselves from family or friends, for whatever reason, should be able to expect that the privacy of their personal information will be respected, particularly where no suspicious or criminal activity is apparent.

21. The proposed changes in Schedule 3 of the Bill are designed to amend the TIA Act to allow an authorised officer of the Australian Federal Police (AFP) or State based Police Forces (State Police) to obtain telecommunications data in circumstances where the authorised officer is satisfied it is reasonably necessary for the purposes of finding a person who the AFP or State Police have been notified of as missing. The Explanatory Memorandum of the Bill states the function of locating a missing person relates to public safety rather than investigating criminal activity.[15]

22. The Office is of the view that authorising the disclosure of telecommunications data for public safety purposes represents an expansion in the scope of the TIA Act and should be carefully considered. The interception of communications between individuals is inherently privacy invasive and generally individuals expect their private conversations, including those via telecommunications systems, to be free from intrusion. At present, this is reflected in the TIA Act, which only allows the interception and the authorised disclosure of telecommunications data in limited circumstances for law enforcement and national security purposes.

23. The Office is concerned that, if the purposes for which telecommunications data can be disclosed is extended to public safety purposes in this instance, then in the future other additional public safety purposes may be identified as warranting a similar approach. Over time this could lead to 'function creep' potentially diminishing privacy protections surrounding communications between individuals.

[14] ALRC Recommendation 34-1.

[15] See page 15 of the Explanatory Memorandum of the Telecommunications Interception and Intelligence Services Legislation Amendment Bill 2010.

24. To minimise the risks associated with function creep the Office recommends that strict privacy protections be put in place when telecommunications data is used or disclosed for the purposes of locating a missing person. The Office acknowledges the Bill has sought to do this by imposing more stringent protections for missing person authorisations, but suggests further amendments could be made to enhance these privacy safeguards.

25. These enhancements could reflect the Australian Government's First Stage Response to the recommendations made by the ALRC in its report in relation to missing persons. In its response the Australian Government stated that an express exception to the use and disclosure privacy principle should apply for the purpose of locating a reported missing person. However, in recognition of the sensitivities associated with missing persons and the need for agencies and organisations to exercise discretion in certain circumstances, the Australian Government indicated that any missing persons exception should be in accordance with binding rules issued by the Privacy Commissioner.[16]

26. The Australian Government's position in relation to missing persons is reflected in the Exposure Draft of the Australian Privacy Principles (APPs) tabled in the Senate on 24 June 2010.[17] The Exposure Draft is currently the subject of a Senate Committee inquiry.[18]

27. The Office suggests consideration be given to introducing a similar set of binding rules or regulations to apply to the handling of telecommunications data related to missing persons. This would promote a nationally consistent approach to personal information handling practices associated with locating missing persons and reduce the potential for fragmentation and gaps in privacy protections that may arise from information being handled in different jurisdictions.

[16] See page 53 of the 'Enhancing National Privacy Protection' the Australian Government's First Stage Response to the ALRC Report, October 2009, available at: http://www.dpmc.gov.au/privacy/reforms.cfm.

[17] See APP 6 (2) (g) in the Exposure Draft of the APPs. The Exposure Draft can be found at: http://www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/guide/exposure_draft.pdf.

[18] The Exposure Draft was referred to the Senate Finance and Administration Committee. The Committee is currently conducting an inquiry into the Exposure Draft of Australian Privacy Amendment Legislation. It is due to report its findings on the first stage of the inquiry by the end of the second sitting week in 2011. The final report is due by 1 July 2011.

Consistent terminology

28. The terminology used in Schedule 3 of the Bill differs slightly to the terminology used in the Exposure Draft for the APPs in APP 6(2)(g)(i). In particular, Items 3, 5 and 7 of Schedule 3 refer to 'finding' a missing person whereas in APP 6 (2)(g)(i) the term 'locate' is used. Similarly, Items 3, 5 and 7 of Schedule 3 refer to a person who has been 'notified' as missing whereas APP 6(2)(g)(i) refers to a person 'reported' as missing. The Office notes it is preferable for consistent terminology to be used when referring to missing persons in both the APPs and the TIA Act to ensure there is a uniform approach to missing persons.

29. In the OPC's submission to the Senate Committee inquiry into the Exposure Draft of the APPs the OPC recommended that the word 'reasonably', used throughout the draft APPs to qualify 'necessary', should be removed. The OPC supported the ALRC's view that 'necessary', on its own, already implied an objective test.[19] Further, the OPC suggested that a plain reading of 'reasonably necessary' may be thought to lower the existing levels of protection in the Privacy Act. The Office acknowledges the term 'reasonably necessary' is referred to elsewhere in the TIA Act but submits there is merit in considering a similar argument for the removal of the word 'reasonably' to qualify 'necessary' in Schedule 3 of the Bill. In any event, the Office notes it is preferable for consistent terminology to be used when referring to missing persons in both the APPs and the TIA Act.

Secondary uses and disclosures of missing person information

30. Under section 182(1) of the TIA Act any unauthorised secondary uses or disclosures of telecommunications data are generally prohibited unless one of the exceptions in section 182 (2) and (3) are met. Items 5 and 7 in Schedule 3 of the Bill propose amending section 182 of the TIA Act by inserting new exceptions into this general prohibition that will apply in circumstances where the secondary use or disclosure is for the purpose of locating a missing person.

[19] The OPCs submission on the Exposure Draft to the APPs is available at: http://www.privacy.gov.au/materials/types/submissions/view/7125.

31. The Bill's proposed new section 182 (2A)(b) will permit the disclosure of information to the person who notified the AFP or the State Police of the missing person (notifying person) in certain circumstances including:

    (i) where the missing person consented to the disclosure, or

    (ii) the missing person is unable to consent, and the disclosure is reasonably necessary to prevent a threat to the missing person's health, life or safety, or

    (iii) the missing person is dead.

32. From a privacy perspective, it is important that individuals are made aware of the ways in which their personal information will be handled so that, to the greatest extent possible, individuals maintain a measure of control over their personal information. In the Office's view, if an individual has the legal capacity to decide how their personal information should be handled, their wishes should be respected. For this reason, the Office supports secondary disclosures to the notifying person of missing person information when consent has been obtained as this is consistent with good privacy practices.

33. It is always preferable, in order to minimise any privacy risks, for express consent to be given by an individual to the disclosure of personal information. However, in circumstances where this is not possible, an individual's consent to the use or disclosure of personal information can be implied. The Office notes the Explanatory Memorandum to the Bill does not give any detailed guidance on issues surrounding consent such as determining capacity and establishing whether implied consent was obtained. Given the complexity and sensitivity associated with missing persons the Office suggests consideration be given to providing more detailed guidance around these issues in the Explanatory Memorandum to the Bill or in any binding rules or guidelines that are developed.

34. The proposed new section 182(2A)(b)(ii) allows secondary disclosures to the notifying person if the missing person is unable to consent and the disclosure is reasonably necessary to prevent a threat to the missing person's health, life or safety. The Office again reiterates the comments in paragraph 29 above that there is merit in considering the removal of the word 'reasonably' to qualify 'necessary' in Schedule 3 of the Bill. Further, the Office is of the view the 'prevent a threat' threshold referred to in this subsection may set a lower standard for disclosures. The Office suggests inserting 'serious' before the word 'threat'. This would raise the standard required before a disclosure could be made and is reflective of the approach taken in the use and disclosure principle in the Exposure Draft of the APPs.[20]

[20] APP 6(2)(c)(i).

35. The Office also recommends the proposed new section 182(2A)(b) of the Bill expressly stipulate that any disclosures to the notifying person be limited to 'evidence of life' information. Disclosing 'evidence of life' information, which only reveals a certain communication took place, is qualitatively different to disclosing all the details relating to the communication such as the location, date and time on which the communication occurred. This Office is of the view, 'evidence of life' disclosures are preferable as they will limit the privacy risks associated with disclosing to a notifying person a missing person's personal information, particularly in circumstances where the missing person was unable to give consent.

Review mechanism

36. The Office welcomes amendments in Schedule 3 of the Bill that ensure enforcement agencies will have an obligation to annually report on the number of authorisations made in relation to missing persons information.[21] Accountability mechanisms such as this will assist in establishing clear and transparent arrangements for the handling of telecommunications data for the purposes of locating missing persons as well as promote community trust and confidence in the proposal.

37. The Office suggests including in Schedule 3 of the Bill a statutory review mechanism that would allow the missing person provisions in the TIA Act to be reviewed and assessed after a period of time. This would augment the existing accountability mechanisms contained in the TIA Act and may be seen as a means of enhancing public trust and confidence in this aspect of the proposal.

38. The review could consider issues such as the suitability of the privacy safeguards in place to protect the personal information of missing persons, the appropriateness of the secondary uses or disclosures of missing person information, and the overall effectiveness of the proposed amendments in pursuing the policy intent behind the proposal.

Schedule 4 – Stored Communication Warrants

39. Schedule 4 of the Bill seeks to amend the TIA Act to clarify that a stored communication warrant can be issued to access the stored communication of a victim of a serious contravention. Section 5E of the TIA Act defines a 'serious contravention' to include a contravention of a law of the Commonwealth, State or Territory that is a serious offence or an offence punishable by imprisonment for a period of at least 3 years.

[21] See Item 8 in Schedule 3 of the Bill.

40. The Explanatory Memorandum to the Bill explains that Schedule 4 seeks to rectify the ambiguity in the current drafting of section 116 of the TIA Act. The proposed amendments in Schedule 4 will allow a stored communication warrant to be issued in relation to a victim of a serious contravention if the person is unable to consent or it is impracticable to gain the person's consent.

41. The Office supports the policy intention behind the proposed amendments in Schedule 4, but suggests guidance be developed to assist law enforcement agencies determine when a person is unable to consent or when it may be impracticable to gain the consent. The Office also suggests the Explanatory Memorandum to the Bill expressly canvass where privacy issues may arise within the context of the proposed amendments. This may assist the issuing authority when considering the factors set out in section 116(2) of the TIA Act.[22]

Schedule 6 – Co-operation, assistance and communication between intelligence agencies

42. Schedule 6 of the Bill proposes amendments to the ASIO Act and the IS Act in order to facilitate greater cooperation, assistance and information sharing between Australia's intelligence agencies including ASIO, ASIS, DSD, and DIGO. Cooperation and assistance between intelligence and law enforcement agencies will also be permitted under the proposed amendments in Schedule 6.

43. The Office believes it is crucial for any regulatory framework setting out information sharing arrangements between intelligence and law enforcement agencies to 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. This can be seen as particularly important in the present circumstance given that the intelligence agencies referred to in the Bill, and information flows between these agencies and other State and Commonwealth law enforcement authorities, fall outside the jurisdiction of the Privacy Act and may be subject to inconsistent privacy frameworks. [23]

[22] Section 116(2) of the TIA Act sets out a range of factors an issuing authority must have regard to when determining whether to issue a warrant. As set out in section 116(2)(a) this includes how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant.

[23] In addition, the Office notes the type of information covered under the proposed amendments would not fall within the IS Act's definition of 'intelligence information' and, for this reason, would not be covered by any Privacy Rules made pursuant to section 15 of the IS Act.

44. To overcome potential gaps in privacy protection the Office recommends that an appropriate privacy framework be put in place to support the information sharing arrangements set out in Schedule 6 of the Bill. This would enhance accountability measures and improve transparency and public confidence in information handling processes under the proposed reforms. The OPC has previously expressed the view that a transparent, published framework clarifying the inter jurisdictional sharing of personal information within Australia by intelligence and law enforcement agencies would be a welcome addition to the public's understanding of what, when and how information is shared. This would also clarify the accountability mechanisms in place.[24]

45. Information handling practices and guidelines that incorporate principles similar to those contained within the Privacy Act could be developed under this framework and established through the development of memoranda of understanding or agreements between jurisdictions. The framework could include the collection, use, disclosure, accuracy, complaint handling, storage, security, retention and destruction of personal information that falls within the scope of the information sharing arrangements**.**

46. The Office notes that such an approach would reflect the ALRC's recommendation that an inter-jurisdictional framework for the sharing of personal information within Australia by intelligence and law enforcement agencies be developed.[25] It would also be consistent with the ALRC's recommendation in its report to develop consistent privacy rules and guidelines for intelligence agencies.[26] The Australian Government will consider both of these ALRC recommendations in its second stage response to the ALRC report.

47. The Office also suggests that consideration be given to including a statutory review mechanism that would allow the operation of the information sharing arrangements to be reviewed and assessed after a period of time. This would enhance the accountability and transparency of the information sharing arrangement embodied in the Bill and may enhance public trust and confidence in this aspect of the proposed amendments.

[24] See page 266 of the OPC's submission to the ALRC Review of Privacy – Discussion Paper 72 in December 2007 and the OPC's Submission to the Parliamentary Joint Committee on the Australian Crime Commission regarding its inquiry into the 'Future impact of serious and organised crime on Australian Society' in August 2007.

[25] ALRC Recommendation 14-2.

[26] ALRC Recommendation 34-1.

Attachment A:

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?