Australian Government

Office of the Privacy Commissioner

Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009 [Provisions]

Submission to the Senate Legal and Constitutional Affairs Committee

August 2009

Key Recommendations

1. The Office of the Privacy Commissioner (the Office) welcomes the opportunity to provide a submission to the Senate Standing Committee on Legal and Constitutional Affairs ('the Committee') regarding the proposed Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009 ('the Bill').

2. The Office makes the following recommendations:

   - In relation to applications for unexplained wealth orders, consideration could be given to the authorised officers having to demonstrate to the court that they have 'reasonable grounds to believe' rather than 'reasonable grounds to suspect'. Requiring a higher level of knowledge would lessen the possibility that personal information is collected from individuals who have not committed any offences

   - Consistent with recommendation 1 of the Sherman Report, the Office believes that the purposes for disclosure of information acquired in any way under the *Proceeds of Crime Act 2002* should be limited to the investigation and prevention of serious offences

   - Disclosures of personal information overseas for the purposes of criminal investigations should relate to offences that would be considered serious if they were committed in Australia

   - To ensure that the community's expectations of both operational effectiveness and appropriate protections for privacy are balanced, measures in the Bill could be assessed against the Office's 'Privacy framework for assessing and implementing new law enforcement and national security powers' (the 4A framework)

   - Consideration could be given to including a formal review mechanism of the new measures within the Bill.

Office of the Privacy Commissioner

1. The Office is an independent statutory body whose purpose is to promote and protect privacy in Australia. The Office, established under the *Privacy Act 1988* (Cth) (''the Privacy Act'), has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT Government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses.

Privacy Act Coverage

2. 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.
3. A number of Australian Government agencies are exempt from the Privacy Act, including defined intelligence agencies and the Australian Crime Commission. Other agencies that may have a role in relation to serious and organised crime such as the Australian Federal Police and the Australian Customs Service, are covered by the Privacy Act.

Background

4. The Office understands that the Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009 ('the Bill') seeks to amend a number of acts to implement a comprehensive national response to combat organised crime. The Office further understands from the Explanatory Memorandum to the Bill[1] that many of the amendments in the Bill have been proposed in response to recommendations from the 2006 Sherman Report.[2]
5. The Office recognises the need for such a response and to improve the ability of law enforcement agencies to target persons deriving financial benefits from organised criminal activity. The Office also notes that the proposed amendments may increase the amount of personal information collected, used and disclosed for these purposes. The Office has previously commented on the development and review of criminal laws including the reform of anti-money laundering and counter-terrorism financing laws.[3]
6. The Office welcomes the opportunity to provide comments to the Committee on the Bill and would like to draw the Committee's attention to some issues regarding the Privacy Act and privacy best practice.

[1] Explanatory Memorandum p 25

[2] *Proceeds of Crime Act 2002* - Report on the Independent Review of the Operation of the Proceeds of Crime Act 2002 by Mr Tom Sherman AO (tabled in Parliament on 18 October 2006). The Office's submission to that review is available at: http://www.privacy.gov.au/publications/sub_proceeds_of_crime_act_200605.html

[3] All previous Office submissions are available at: http://www.privacy.gov.au/materials/types/submissions?sortby=65

Key issues for privacy and crimes legislation

7. The Office's previous submissions in relation to crimes legislation share a number of common themes, including that:

   - privacy is an important right, the protection of which helps to promote community trust and confidence in public administration and law enforcement
   - it may be necessary to balance privacy interests with other important public interests, such as community safety and security
   - an expansion in the power of law enforcement and intelligence agencies to collect, use and disclose personal information about individuals may affect the privacy of individuals especially when personal information is obtained through mandatory orders or other similar powers. In that regard, any lowering of privacy protections for law enforcement purposes should be:
     - a necessary response to a clearly defined problem
     - proportionate to the risk posed, and
     - accompanied by adequate accountability and review mechanisms.

8. In the Office's view, these themes also apply to the Bill. Following are some specific suggestions in relation to the Acts being amended by the Bill.

Proceeds of Crime Act

Unexplained Wealth Amendments

9. The *Proceeds of Crime Act 2002* (PoC Act) currently contains a number of measures to assist in the investigation of matters related to the proceeds of crime. These measures include: examination orders, production orders, notices to financial institutions, monitoring orders and search warrants.

10. The Bill would add to the PoC Act and the existing Commonwealth criminal assets confiscation regime by establishing unexplained wealth orders, which require a person to attend court for the purpose of enabling the court to decide whether to make an order against the person where wealth cannot be shown to have been lawfully acquired.[4]

11. According to the Bill's Explanatory Memorandum ('EM'), existing confiscation mechanisms are not always effective, as most of them require a proven link to be made between the individual and the commission of an offence. In cases where individuals are suspected of involvement with organised crime, it is not always possible to link them directly by evidence to the commission of specific offences.[5]

12. Under the provisions, before a court proceeds with a hearing for an unexplained wealth order, it will assess whether the authorising officer has demonstrated

[4] *Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009*, Item 13 – inserts new Part 2-6 into Chapter 2 of the PoC Act which will add unexplained wealth orders to the confiscation processes of the Act.

[5] *Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009*, Explanatory Memorandum pp.2, 7

reasonable grounds to suspect that the total value of the person's wealth exceeds the value of the person's wealth that was lawfully acquired[6]. An unexplained wealth order would give investigators significant powers to gather personal information about suspected individuals from a number of sources, such as financial institutions.

13. Item 38 of the Amendment Bill would amend the definition of 'suspect' in section 338 of the PoC Act to include a person, in relation to an unexplained wealth order, whose wealth is suspected of exceeding the value of wealth that was lawfully acquired.

14. The Office welcomes the inclusion of judicial oversight for the issuing of unexplained wealth orders and believes that independent oversight should help to minimise the possible adverse impacts on individuals who have not committed any offence. However, given the scope of powers and the increased risk that personal information could be collected from such individuals, the Office believes that consideration could be given to the authorised officers having to demonstrate to the court a level of knowledge that is higher than 'reasonable grounds to suspect. The Office suggests that authorised officers could instead be required to demonstrate 'reasonable grounds to believe'.[7]

Sharing and Disclosing Information

15. The Office supports measures that would improve the ability of law enforcement agencies to target individuals who derive financial benefit from organised crime.[8] However this should be balanced against the need to protect the privacy of individuals whose personal information is collected and used by law enforcement agencies. This is especially important considering that these amendments are directed towards collecting information about individuals that may not be linked by evidence to the commission of an offence.[9]

16. Agencies subject to the Privacy Act are permitted to disclose personal information in accordance with exceptions to IPP 11. These exceptions include where the disclosure is for the enforcement of criminal law[10] and where the disclosure is required or authorised by or under law. [11]

    The Office notes that the Amendment Bill inserts a new Part 3-6 into the PoC Act which specifically authorises the disclosure of information obtained under the PoC Act, to certain authorities for certain purposes.[12] The Office notes that these purposes are quite broad and they relate to information that has been obtained in various ways including as a result of mandatory examination.

17. The Sherman Report recommended that "information acquired in any way under the [PoC] Act relating to any serious offence can be passed to any agency having a lawful function to investigate that offence".[13] The Office understands that Part 3-

[6] Amendment Bill, section 179B
[7] An example of this form of words can be found in the Bill under Schedule 3 clause 15HT which requires the Ombudsman to have "reasonable grounds to believe"
[8] EM, p. 2
[9] EM, p. 2
[10] See IPP 11.1(e)
[11] See IPP 11.1(d)
[12] Amendment Bill, Item 67
[13] Sherman Report, Recommendation 1

6 was intended to effect the changes necessary to achieve this outcome.[14] In order to accurately reflect this recommendation, the Office believes that the purposes for disclosure should be limited to the investigation and prevention of serious offences.

Disclosures overseas

18. The Office is aware that these provisions would also apply in disclosing information to a law enforcement authority in a foreign country.[15] As noted in its submission to the Attorney-General's Department's Review of Extradition Arrangements, the Office believes that allowing personal information flows to foreign countries for the purposes of enforcing foreign laws pose particular privacy risks in that the information may relate to conduct that is lawful in Australia. This would create an inconsistency in Australian privacy regulation, by allowing personal information flows offshore that are not permitted onshore. [16]

19. To balance this process and meet community expectations, the Office believes that disclosures should not be made unless the offence under investigation overseas would also be considered a serious offence had it occurred in Australia.

20. In addition, where privacy protections substantially similar to the IPPs are not in place in an overseas country, Australian agencies should establish administrative arrangements or memoranda of understanding or protocols with the overseas authority regarding appropriate handling practices when handling personal information for the permitted purposes.

Telecommunications (Interception and Access) Act

21. In recent years, the Office has made a number of submissions concerning telecommunications interception powers.[17] The Office is of the view that any proposal which broadens telecommunications interception powers should consider the following:

- all private conversations conducted over the telecommunications system, whether by telephone, internet chat, email, SMS, or other telecommunication means, should, wherever practicable, be afforded an equivalent level of privacy protection
- extension of the coverage of the TIA Act requires robust reporting requirements to ensure transparency and to allow for the ongoing monitoring of the operation of new powers and
- information collected by telecommunications interception should be used only for the purpose originally intended, unless there are cogent public policy reasons which reflect community expectations.

[14] EM, p. 25; Sherman Report, Chapter 4
[15] Clause 266A(2), Crimes Legislation Amendment (Serious and Organised Crime) Bill 2009
[16] Submission available at: http://www.privacy.gov.au/materials/types/submissions/view/6680#mozTocId183262
[17] See 'Review of the Regulation of Access to Communications under the *Telecommunications (Interception) Act 1979'* (June 2005) available at www.privacy.gov.au/publications/tiasub.pdf. and *Telecommunications (Interception and Access) Amendment Bill 2008*; Submission to the Senate Legal and Constitutional Affairs Committee (April 2008) available at: http://www.privacy.gov.au/publications/sub_tele_interception_bill0408.html

22. The Office welcomes the intent of the EM in stating that the proposed amendments recognise the invasive nature of telecommunications interception and ensure that the community's expectations of both operational effectiveness and appropriate protections for privacy are balanced.[18]

Data Retention

23. The Office notes that Bill does not contain provisions regarding the retention or disposal of data. While the IPPs do not require the disposal or destruction of data, the best privacy practice is for agencies to dispose of or destroy data when it is no longer necessary or relevant. The indefinite retention of personal information could lead to this information becoming inaccurate or incomplete. Given the important law enforcement decisions that could be made using such data, it is important to maintain its quality by removing obsolete or irrelevant information.
24. The Office suggests that agencies that have wide collection powers should also develop retention and disposal policies, especially in relation to personal information. By doing so, agencies will improve the quality of their data holdings and ensure that they make decisions using the highest quality information available. Agencies covered by the Privacy Act generally should not use personal information unless they take steps to see that is accurate, up-to-date and complete.[19]

The 4A framework

25. The Office recognises that it is often necessary to balance privacy with other important social interests, such as the safety and security of the community. As one means of making judgements between competing priorities, the Office has developed and refined a tool called the '4A framework' (see Attachment 1).
26. The 4A framework has been designed to assist agencies consider privacy 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 they are:
    - necessary and proportional to address the immediate need and
    - are subject to appropriate and ongoing accountability measures and review.
27. In accordance with the 4A framework the Office suggests that mechanisms to ensure such periodic review could be built into the Bill. These mechanisms might include a parliamentary review after a fixed period.

[18] EM, p.143
[19] see IPP 8 available at http://www.privacy.gov.au/materials/types/infosheets/view/6541#h

Attachment 1: Privacy framework for assessing and implementing new law enforcement and national security powers

The Office of the Privacy Commissioner has a 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?