Australian Government

Office of the Privacy Commissioner

Telecommunications (Interception and Access) Amendment Bill 2008

Submission to the Senate Legal and Constitutional Affairs Committee

April 2008

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner (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, all large private sector organisations, health service providers and some small businesses. The Office also has responsibilities under the Privacy Act in relation to credit worthiness information held by credit reporting agencies and credit providers, and personal tax file numbers used by individuals and organisations.

Background

2. The Office welcomes the opportunity to make these comments to the Senate Legal and Constitutional Committee ('the Committee') on *Telecommunications (Interception and Access) Amendment Bill 2008* (the TIA Bill).

3. A primary policy objective of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) is to protect the privacy of individuals who use the Australian telecommunications system. The TIA Act specifies the circumstances in which it is lawful for law enforcement agencies and the Australian Security Intelligence Organisation (ASIO) to intercept communications under the authority of a warrant, subject to reporting and accountability mechanisms.

4. The Office agrees with the first finding of Mr Anthony Blunn's AO 2005 *Report of the Review of the Regulation of Access to Communications* ('the Blunn Review'), that:

> "The protection of privacy should continue to be a fundamental consideration in, and the starting point for, any legislation providing access to telecommunications for security and law enforcement purposes".[1]

5. At the same time, this Office recognises the need to ensure an appropriate balance between the public interest in maintaining privacy and the ability of law enforcement and national security agencies to undertake their legitimate functions.

6. The Office notes that in recent years there has been a number of amendments to the regulation of telecommunications interception. These amendments have resulted in an incremental expansion in powers regarding interception. Accordingly, the Office suggests that the amendments now proposed in the TIA Bill could usefully be considered with regard to this broader context.

[1] A S Blunn AO *Report of the Review of the Regulation of Access to Communications*, August 2005, p.5, available at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~xBlunn+Report+13+Sept.pdf/$file/xBlunn+Report+13+Sept.pdf.

Framework for considering new law enforcement or national security powers that may impact on privacy

7. To assist agencies and others in their consideration of competing priorities, such as privacy and security, the Office has developed and refined a framework by which new legislative measures can be assessed.
8. 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.
9. This framework is attached and the Office commends the framework to the Committee when it is considering the TIA Bill.

Matters considered in this submission

10. The Office has considered two elements of the TIA Bill, these being:
    - the proposed extension of sunset provisions relating to 'network protection provisions'; and
    - the proposed amendments to allow named person warrants to apply to 'multiple telecommunication devices' (rather than 'a particular telecommunications device' as is currently allowed).
11. The Office has not commented on the amendments relating to the reporting requirements under the TIA Act.

Previous submissions

12. In the recent years, the Office has made a number of submissions concerning telecommunications interception powers. The issues raised in these submissions include that:
    - 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;[2]
    - extension of the coverage of the TIA Act to a broader range of agencies, requires robust reporting requirements to ensure transparency and to allow for the ongoing monitoring of the operation of the new stored communications regime;[3]

[2] Submission made June 2005 'Review of the Regulation of Access to Communications under the *Telecommunications (Interception) Act 1979',* available at www.privacy.gov.au/publications/tiasub.doc.
[3] ibid

- the need for clarity in regard to the operation of device based warrants;[4]
- the need for positive obligations on law enforcement agencies to destroy irrelevant material containing personal information collected through voluntary disclosure;[5] and
- the operation of the TIA Act should be subject to an independent review at least every five years.[6]

The TIA Bill

Extension of sunset provisions relating to 'network protection provisions'

Current provisions

13. Subsections 5F(2) and 5G(2) of the TIA Act currently provide Commonwealth and state law enforcement and security agencies with exemptions to the general prohibitions on listening to or copying communications 'passing over the telecommunications system'.

14. These exemptions allow law enforcement and security agencies to monitor communications through their network for the purpose of protecting and maintaining their network and professional standards.

15. The exemptions are currently subject to two-year sunset provisions and are scheduled to cease to have effect in June 2008. The sunset provisions were intended as an interim measure to ensure agencies' network protection systems are not in breach of the TIA Act, pending the development of more comprehensive legislation.

16. These provisions were made to give effect to findings of the Blunn Review, which recommended that:

> "...access to communications without warrant be permitted where it is necessarily incidental to the protection of data systems or the authorised development or testing of new technologies or interception capabilities."[7]

17. The Blunn Review also recommended that this access be "...subject to appropriate controls".

Proposed amendments to the sunset provisions

18. Schedule 1 of the TIA Bill seeks to extend the operation of the sunset provisions by a further 18 months.

---

[4] In March 2006, the Office made a submission to the Committee's inquiry into the provisions of the Telecommunications (Interception) Amendment Bill (2006), available at http://www.privacy.gov.au/publications/subtel0207.pdf

[5] In July 2007, the Office made a submission to the Committee's inquiry into the Telecommunications (Interception and Access) Amendment Bill 2007, available at http://www.privacy.gov.au/publications/subcommtiabill190707.html.

[6] ibid

[7] A S Blunn AO *Report of the Review of the Regulation of Access to Communications*, August 2005, p.62, available at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~xBlunn+Report+13+Sept.pdf/$file/xBlunn+Report+13+Sept.pdf.

19. In stating the need for the extension of the sunset period for network protection provisions, the Explanatory Memorandum for the TIA Bill states:

> "The main purpose of Schedule 1 is to extend the operation of the sunset provisions to enable the development of a full legislative solution that clarifies the basis on which network administrators may access communications within their network for the purposes of network security and the enforcement of professional integrity."

20. The network protection exemptions were inserted by the TIA Amendment Act 2006 and initially only applied to the Australian Federal Police. The 2007 amendments to the TIA Act extended this to cover more than twenty Commonwealth and state/territory law enforcement and security agencies, as defined by subsection 5(1) of the Act.

21. The Office is not aware of the degree of progress that has been made to establish a more permanent legislative solution.

Necessity for exemptions to be accompanied by appropriate controls

22. The Blunn Review recognised the problem faced by network administrators accessing communications for the purpose of ensuring network security and the need for measures that would clarify that protective activities would not breach the TIA Act.

23. However, the Mr Blunn also noted that:

> "...from a privacy point of view, uncontrolled access is simply not satisfactory".

24. The Review report went on to state that:

> "An access regime should be established which provides for appropriate protections and prevents back-door use and access to obtain consent. Those protections should... restrict access to that required for the identified purpose i.e. the protection of the system. There should be clear authorisation and the persons with the authority should be clearly identified. Those persons should be required to protect the privacy of any data in the same way that the employees of C/CSPs [respectively, 'carriers' and 'carriage service providers'] are required to protect data accessed in the course of their employment"

25. The Office supports the position of the Blunn Review that network protection provisions should be accompanied by appropriate privacy protections. Further, in the view of the Office, the subsequent widening of the scope of the network protection exemption to over 20 agencies makes it more important that the safeguards recommended by the Blunn Review are built-into the legislation, including for the purposes of the proposed 18 month extension to the sunset provisions.

26. The Office recommends that consideration be given to amending the TIA Bill to contain more rigorous parameters around the network protection provisions including:

    a) a prohibition on secondary use of any data accessed for the purpose of protecting the agency's network security, unless there are cogent public policy reasons which reflect community expectations;

    b) that agencies must clearly identify the people who are given the authorisation under the exemptions; and

c) that any data obtained for the purpose of network security should be immediately destroyed when it is no longer needed for that purpose.

Amendments to device-based named-person warrants

Proposed amendments

27. Section 9A of the TIA Act allows the Director-General of Security to apply to the Attorney-General for the issue of named person warrants in regard to individuals who are "engaged in, or likely to be engaged in, activities prejudicial to security." Named person warrants can apply to either telecommunications services being used by a particular person (s 9A(b)(i)), or 'a particular telecommunication device' (s 9A(b)(ii)).

28. A number of the proposed amendments seek to allow named person warrants to apply to multiple telecommunication devices, rather than a 'particular telecommunication device'.

29. The proposed changes will allow agencies to intercept '*any* telecommunication device that the person is using or is likely to use' (emphasis added).

30. As proposed under subsection 9A(2)(ba) the Director-General of Security must, in applying for a named-person device warrant, provide details "to the extent these are known to the Director-General of Security" sufficient to identify the telecommunication devices that the person is using or is likely to use. Consequently, under this amendment, neither the application nor the warrant will need to exhaustively list the telecommunication devices that may be intercepted.

31. Similar amendments are proposed for s11B, which provides for the Director-General of Security to apply for named person warrants for the purpose of obtaining foreign intelligence relating to a matter specified in the warrant.

Need for specificity and oversight in device warrants

32. The Explanatory Memorandum to the TIA Bill describes the amendments relating to named-person warrants as being technical in nature because they are consistent with the provisions governing service-based named person warrants.

33. In the Office's view, the proposed amendments may diminish privacy safeguards provided by the warrant process.

34. The additional devices will not be subject to the specific independent scrutiny of the Attorney-General (as prescribed decision maker) as the amendments could allow additional devices to be intercepted which were not expressly included in the application. This could reduce the oversight role of the warrant authorisation process in safeguarding against errors and potentially unjustified invasion of a person's privacy.

35. In its submission to the review of the TIA Act conducted by Mr Tom Sherman AO (June 2003), the Office expressed similar concerns about

changes made to the Act in 2000 which permit agencies to intercept additional services that are not identified in the warrant:

> It is clear that the degree of independent scrutiny of services to be intercepted and the safeguards in place to prevent the unnecessary interception of services vary according to whether the service is identified before or after the warrant is issued.[8]

Unreliable nature of existing device identification systems

36. In the Office's view, aligning the rules governing device warrants with those that apply to service warrants introduces a greater risk of intrusion into the privacy of individuals about whom there may be no cause for suspicion. This is because of the unreliable nature of existing telecommunication device identification systems, which make it uncertain whether telecommunication interceptions could be conducted in regard to a specified device.

37. The provisions relating to device-based warrants introduced into the TIA Act in 2006 were designed to gain access to an individual piece of equipment, such as a computer or mobile phone, via a unique identification number.

38. However, the Committee's report into the 2006 TIA Bill highlighted the difficulties of accurately identifying a person through the use of International Mobile Service Identifiers (IMSI) or other similar identification numbers.

39. During the inquiry, in response to questioning from the Committee about the introduction of device-based warrants, the Australian Federal Police (AFP) stated that there is the possibility that the unique identifying number for a telephone or computer may get mixed up with other telephones or computers. The AFP stated that:

> "We would make all efforts we could to ascertain that [the unique identifying number] through our enquiries to the telecommunication companies. The concern, of course, is that some of these are fraudulently obtained. A number of different identification numbers can be applied to that communication tool, be it a telephone or a laptop computer."[9]

40. The Committee concluded:

> "…any arrangement designed to target a specific piece of equipment should be able to identify it with a high degree of certainty. It is the Committee's view that while there is a clear operational requirement for law enforcement agencies to be able to target specified devices, doubts remain over their capacity to identify these devices with a high degree of certainty." [10]

41. Accordingly, the Committee recommended:

---

[8] Available at http://www.privacy.gov.au/publications/telsub.pdf

[9] Committee Hansard March 2006, p.77, http://www.aph.gov.au/hansard/senate/commttee/S9205.pdf

[10] The Senate Legal and Constitutional Legislation Committee, Provisions of the Telecommunications (Interception) Amendment Bill, March 2006, p. 51, available at: http://www.aph.gov.au/SENATE/COMMITTEE/legcon_ctte/ti/report/report.pdf

> "That the recommendation contained in paragraph 3.2.5 of the Blunn report be adopted, and priority given to developing a unique and indelible identifier of the source of telecommunications and therefore of access."[11]

42. The Office notes that neither the Committee's concerns, nor the acceptance of the recommendation of the then Government, are acknowledged in the Explanatory Memorandum to the TIA Bill.

43. In the Office's view, establishing an interception regime for a range of unspecified devices is problematic where it cannot be reasonably assured that the relevant device will relate to a relevant individual.

44. The Office recommends that the proposed amendments relating to device-based warrants be modified to require that:

    a) while a single warrant may authorise interception of telecommunications made by means of multiple devices, each of those devices must be named on the warrant;

    b) the issuer of the warrant must be satisfied that:

        i. each of those devices is used or likely to be used by the named person; and

        ii. each device can be uniquely and accurately identified for the purpose of interception.

Key Recommendations

45. The Office makes the following key recommendations in regard to the proposed Amendment Bill:

    a) That the TIA Bill contain more rigorous parameters around the interim 'network protection provisions' including:

        - strict prohibition on secondary use of any data accessed for the purpose of protecting the agency's network security, unless there are cogent public policy reasons which reflect community expectations;
        - that agencies must clearly identify the people who are given the authorisation under the exemptions;
        - that any data obtained for the purpose of network security should be immediately destroyed when it is no longer needed for that purpose.

    b) That the proposed amendments relating to device-based warrants be modified to require that:

        - while a single warrant may authorise interception of tele-communications made by means of multiple devices, each of those devices must be named on the warrant;
        - the issuer of the warrant must be satisfied that:

[11] Ibid

i) each of those devices is used or likely to be used by the named person; and

ii) each device can be uniquely and accurately identified for the purpose of interception.

46. The Office reiterates its view that the operation of the TIA Act should be subject to overall independent review at least every five years.[12]

[12] See, for example, the Office's submission to the Inquiry by the Senate Standing Committee on Legal and Constitutional Affairs into the *Telecommunications (Interceptions and Access) Amendment Bill 2007,* available at http://www.privacy.gov.au/publications/subtel0207.pdf

Attachment 1: 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?