Parliament of Australia
Department of Parliamentary Services

Parliamentary Library
Information analysis and advice for the Parliament

BILLS DIGEST

7 March 2008, no. 71, 2007–08, ISSN 1328-8091

Telecommunications (Interception and Access) Amendment Bill 2008

Bronwen Jaggers
Law and Bills Digest Section

Contents

Telecommunications (Interception and Access) Amendment Bill 2008

Date introduced: 20 February 2008

House: House of Representatives

Portfolio: Attorney-General

Commencement: Sections 1 to 3 commence upon Royal Assent. Schedule 1, items 1-19, 26-34, 36, and 38-49 will commence on the day after Royal Assent. Schedule 1, items 20-25, 35 and 37 commence on a day to be fixed by proclamation, or six months after Royal Assent.

Links: The relevant links to the bill, Explanatory Memorandum and second reading speech can be accessed via BillsNet, which is at http://www.aph.gov.au/bills/. When bills have been passed they can be found at ComLaw, which is at http://www.comlaw.gov.au/.

Purpose

To amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to extend the operation of network protection provisions[1] which are due to expire (sunset) on 13 June 2008. The bill also proposes a number of minor technical amendments to the TIA Act.

Background

Under the TIA Act, it is prohibited to intercept, or authorise interception, of a communication passing over a telecommunications system. However, the Act provides a number of exemptions, including to the officers of law enforcement and security agencies under warrant, if the Attorney-General is satisfied that the telecommunications system is being used by a person engaged in, or likely to be engaged in, or reasonably suspected to be engaged in, activities or purposes that are prejudicial to security.[2]

Given rapid changes in communications technology, it has become possible to communicate without a message 'passing over' the telecommunications system. For example, those engaged in terrorist activities may use methods such as storing emails in draft accounts but not sending them, writing mobile phone texts but not sending them,

1. See pages 6-7 for detail on network protection provisions.
2. *Telecommunications (Interception and Access) Act 1979*, Chapter 2.

swapping SIM cards, and using others' telephones to record voicemail messages. Such communications are referred to as 'stored' communications.

In 2004 the then government introduced interim legislation which allowed security and law enforcement agencies access to 'stored' communications using a normal search warrant, rather than a telecommunications interception warrant (which then only applied to communications 'passing over' a system, and not 'stored' communications).

In March 2005 the government appointed Anthony Blunn AO (a former Secretary of the Attorney-General's Department) to undertake a review of the regulation of access to communications under the TIA Act. In August 2005 Mr Blunn completed his report titled *Report of the Review of the Regulation of Access to Communications*.[3] The report, tabled in Parliament on 14 September 2005, recommended that legislation dealing with access to telecommunications data for security and law enforcement purposes be established.

In 2006 the government introduced legislation that responded to the first tranche of the report's recommendations. The *Telecommunications (Interception) Amendment Act 2006* established a warrant regime for access to stored communications, and included some controversial measures such as 'B Party Intercepts'.[4]

The government then implemented the second phase of Blunn recommendations in 2007 with the *Telecommunications (Interception and Access) Amendment Act 2007*. This Act transferred provisions in the *Telecommunications Act 1997* which regulated access to telecommunications data for national security and law enforcement purposes to the TIA Act. The Act also implemented a new two-tier access regime for access to historic and 'prospective' (ie real-time) telecommunications data.[5]

Some of the amendments to the TIA Act contained in the 2006 and 2007 amending Acts included sunset clauses, due to expire on 13 June 2008. This bill seeks to extend those sunset clauses, and to make some technical amendments.

Further detail is provided in the Main Provisions section.

---

3. Anthony Blunn AO, *Report of the Review of the Regulation of Access to Communications*, August 2005, available at the Attorney-General's website: http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~xBlunn+Report+13+Sept.pdf/$file/xBlunn+Report+13+Sept.pdf.
4. See Sue Harris-Rimmer, 'Telecommunications (Interception) Bill 2006', *Bills Digest* no. 102, 2005–06, 28 February 2006, Parliamentary Library, at: http://www.aph.gov.au/library/pubs/bd/2005-06/06bd102.pdf.
5. See Bronwen Jaggers, 'Telecommunications (Interception and Access) Amendment Bill 2007' *Bills Digest* no. 10, 2007–8, 3 August 2007, Parliamentary Library, at: http://www.aph.gov.au/library/pubs/bd/2007-08/08bd010.pdf.

Committee consideration

The Senate Legal and Constitutional Affairs Committee conducted inquiries into the 2006 and 2007 amending Acts to the TIA Act. The reports can be found on the Committee's website.[6] Given that this has been flagged by the Minister as a 'time critical' bill, it is unclear whether this bill will be referred to the Committee for consideration.

Coalition/Australian Democrat/Greens/Family First policy position/commitments

The Opposition and other parties have not made a public statement on the current bill. In the Senate Committee inquiries into the 2006 and 2007 amending bills, the Australian Democrats supported the Committee's recommendations on both bills, but made further recommendations to improve privacy considerations.

Financial implications

The Explanatory Memorandum states that there will be no financial impact from this bill.

Main provisions

Extension of sunset clauses

Items 1 and **2** seek to amend **subsections 5F(3) and 5G(3)** of the TIA Act to repeal the existing sunset provision, which is two years after the 2006 Act's commencement (13 June 2008), and insert a new sunset date of 12 December 2009.

Subsection 5F relates to when a communication is taken to be 'passing over' a telecommunications system. The general tenet of the TIA Act is that interception of a communication that is 'passing over' a telecommunications system is forbidden, except with a telecommunications interception warrant.

However, an exemption is provided to the employees of a number of Commonwealth and state law enforcement and security agencies, if they are responsible for operating, protecting or maintaining a network or if they are responsible for enforcement of the professional standards (however described) of the agency or authority. Subsection 5F is reproduced below.

---

6. Senate Legal and Constitutional Affairs Committee: http://www.aph.gov.au/Senate/committee/legcon_ctte/completed_inquiries/index.htm.

5F When a communication is passing over a telecommunications system

(1) For the purposes of this Act, a communication:
  (a) is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; and
  (b) is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication.

(2) However, if a communication is sent from an address on a computer network operated by or on behalf of:
  (a) a Commonwealth agency; or
  (b) a security authority; or
  (c) an eligible authority of a State;

  the communication is taken not to start passing over a telecommunications system, for the purposes of this Act, until it is no longer under the control of any of the following:
  (d) any employee, member of staff or officer of the agency or authority responsible for operating, protecting or maintaining the network;
  (e) any employee, member of staff or officer of the agency or authority responsible for enforcement of the professional standards (however described) of the agency or authority.

(3) Subsection (2) ceases to have effect at the end of the period of 2 years starting at the commencement of this section.

Similarly, subsection 5G(2) provides an exemption to a number of law enforcement and security agency employees in regard to the intended recipient of a communication:

5G The intended recipient of a communication

(1) For the purposes of this Act, the ***intended recipient*** of a communication is:
  (a) if the communication is addressed to an individual (either in the individual's own capacity or in the capacity of an employee or agent of another person)—the individual; or
  (b) if the communication is addressed to a person who is not an individual—the person; or
  (c) if the communication is not addressed to a person—the person who has, or whose employee or agent has, control over the telecommunications service to which the communication is sent.

(2) In addition to the person who is the intended recipient of a communication under subsection (1), if a communication is addressed to a person at an address on a computer network operated by or on behalf of:
  (a) a Commonwealth agency; or
  (b) a security authority; or
  (c) an eligible authority of a State;

each of the following is also an ***intended recipient*** of the communication for the purposes of this Act:

(d) any employee, member of staff or officer of the agency or authority responsible for operating, protecting or maintaining the network;

(e) any employee, member of staff or officer of the agency or authority responsible for enforcement of the professional standards (however described) of the agency or authority.

(3) Subsection (2) ceases to have effect at the end of the period of 2 years starting at the commencement of this section.

The exemptions, dubbed by the Minister as 'network protection provisions'[7], were inserted by the *Telecommunications (Interception) Amendment Act 2006* and initially only applied to the Australian Federal Police (AFP), although the 2007 amending Act extended this to cover Commonwealth agencies, security authorities and eligible state authorities, as defined by the TIA Act. The exemptions now include:[8]

- **Commonwealth agency** – the AFP, the Australian Commission for Law Enforcement Integrity, or the Australian Crime Commission
- **eligible state agency** – the Police Force of any state, and
  - in NSW: the Crime Commission, the Independent Commission Against Corruption, the Inspector of the Independent Commission Against Corruption, the Police Integrity Commission or the Inspector of the Police Integrity Commission
  - in Victoria: the Office of Police Integrity
  - in Queensland: the Crime and Misconduct Commission
  - in Western Australia: the Corruption and Crime Commission or the Parliamentary Inspector of the Corruption and Crime Commission.
- **security authority** means an authority of the Commonwealth that has functions primarily relating to:
  - security
  - collection of foreign intelligence
  - the defence of Australia, or
  - the conduct of the Commonwealth's international affairs.

---

7. Hon. Robert McClelland MP, Attorney-General, 'Second Reading Speech: Telecommunications (Interception and Access) Amendment Bill 2008', *House of Representatives Debates*, 20 February 2008, p. 5.
8. Subsection 5(1) of the TIA Act 1979.

– According to the Explanatory Memorandum for the 2007 amending Act, a security authority would therefore include ASIO, the Department of Defence, and the Department of Foreign Affairs and Trade.[9]

In stating the need for network protection provisions, the Explanatory Memorandum for this bill states:

> Networks are protected from security risks by the use of gateway control systems. The use of these systems (such as virus protection software) does not generally violate interception legislation. Automated systems can screen and reject incoming communications if they are suspected of containing a virus, and network operators are able to monitor internal and outbound communications (including emails and internet browsing) provided they have obtained the consent of people using the network. However, some network protection activities that take place at the threshold of a network may constitute a technical breach of the TIA Act.[10]

In his report Anthony Blunn recognised the problem faced by network administrators accessing communications for the purpose of ensuring network security:

> Given the 'rights' of owners to protect their system, the potential consequences of not doing so, the universality of the need and the time-critical nature of the required response, it is not in my opinion possible to meet the reasonable needs to protect systems by amending the Interception Act to provide specific exemptions.
>
> However from a privacy point of view uncontrolled access is simply not satisfactory. An access regime should be established which provides appropriate protections and prevents back-door use and access to obtain content. Those protections should in my view 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 that authority should be clearly identified. Those persons should be required to protect the privacy of any data accessed in the same way that the employees of C/CSPs are required to protect data accessed in the course of their employment.[11]

Mr Blunn also recognised the possibility of 'incidental' interception of communications in the course of developing new technologies (in particular, but not limited to, the defence and security agencies). Blunn recommended:

---

9. Explanatory Memorandum: Telecommunications (Interception and Access) Amendment Bill 2007, p. 41, available at: http://parlinfoweb.parl.net/parlinfo/Repository/Legis/oldEms/Linked/31100714.pdf.
10. Explanatory Memorandum, p. 3.
11. Anthony Blunn AO, op.cit, pp. 57–62.

> Subject to appropriate controls, 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.[12]

The network protection provisions were a last-minute government amendment to the Telecommunications (Interception) Amendment Bill 2006. The government stated that the late insertion of the network protection provisions for the AFP (extended in 2007 to a number of other agencies), rather than inclusion in the original bill or during the Senate committee inquiry, was because the AFP had not received final policy approval for the provisions prior to the Parliamentary debate. Because of the lack of time to examine the network protection provisions, the ALP and Australian Democrats opposed the amendments, however they were passed by Parliament. There was no specific mention of why a two-year sunset clause was included, but the Minister did refer to the fact that more comprehensive legislation to deal with the issue would be needed further down the track.[13]

The proposed 18-month extension of the sunset clause in the current Bill is to allow the drafting of a permanent legislative solution to implement the Blunn Report recommendation. In his second reading speech for the bill the Attorney-General stated:

> The proposed 18-month extension of the existing network protection provisions will ensure law enforcement and security agencies can continue to protect their networks while a comprehensive long-term solution is developed. My department has already undertaken extensive work on legislative changes that would implement the Blunn report recommendation. As mentioned, these measures will have implications across government, corporate and private networks. They must also address complex issues associated with privacy, and state and territory laws. It is important not to rush those changes, and there must be enough time to consult widely on their impact. An 18-month extension will enable full consideration of a more complete solution across all networks. [14]

Comment

The proposed extension of the network protection provisions sunset clauses by another 18 months means that over 20 Commonwealth and state/territory law enforcement and security agencies will be given access exemptions until the end of 2009. Blunn noted that unrestricted access is unsatisfactory and recommended an authorisation process – including a requirement that the access is strictly for the purpose of maintaining network security, and that the people who are given authorisation are clearly identified. While the Minister states that resolving the Blunn recommendation is complex and requires separate

---

12. ibid.
13. For the debate on the network protection provisions, see Senate, *Debates*, 26 March 2006, pp. 124-130.
14. Hon. Robert McClelland MP, op.cit.

legislation, it could be possible to insert such authorisation processes into the interim legislation.

Technical amendments

Multiple telecommunications devices

A number of the technical amendments are related to a proposed change to allow named person warrants to apply to 'multiple telecommunications devices', rather than 'a particular telecommunications device' as is currently allowed.

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. Named person warrants can apply to either telecommunications services being used by a particular person, or 'a particular telecommunications device' used or likely to be used by the person.[15]

Item 3 proposes to amend subparagraph **9A(1)(b)(ii)** of the TIA Act to allow a device-based warrant to intercept communications from multiple telecommunications devices.

Under the TIA Act, a telecommunications device is defined as 'a terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system.'[16]

It is useful to note that under the TIA Act, warrants for interception of a telecommunications device are to be used as a 'second stage' measure – only if it would not be practical to intercept the telecommunications services used, or likely to be used, by the person in respect of whom the warrant is to be issued:

> 9A(3): The Attorney-General must not issue a warrant that authorises interception of communications made by means of a telecommunications device identified in the warrant unless he or she is satisfied that:
>
> (a) there are no other practicable methods available to the Organisation at the time of making the application to identify the telecommunications services used, or likely to be used, by the person in respect of whom the warrant would be issued; or
>
> (b) interception of communications made to or from a telecommunications service used, or likely to be used, by that person would not otherwise be practicable.

The Explanatory Memorandum for the 2006 amending Act which introduced these warrants gives the example of a person using multiple SIM cards in a mobile phone in

---

15. Explanatory Memorandum, p. 4.
16. TIA Act, subsection 5(1).

quick succession, making it impractical to access each telecommunications service being used by the relevant person.[17]

Items 4-14 make subsequent amendments to TIA sections 9A, 11B and 16 relating to the change to 'multiple telecommunications devices'.

Items 20-25 amend the Part of the TIA Act relating to warrant applications, to allow an application for 'multiple telecommunications devices' **Items 35 and 37** make related amendments to the need to inform a Managing Director of a carrier to be notified of additional devices to be added to a device-based named person warrant.[18]

Reporting requirements

As a result of changes to the TIA Act brought about by the 2006 and 2007 amending Acts, there is some duplication in the notification and reporting requirements now contained in the consolidated Act. The remaining items in this bill seek to rectify these problems by:

- repealing some now redundant reporting requirements (**items 26-30, 42-48**)
- allowing a 'certifying officer' of an agency (ie SES level or equivalent) to notify the Managing Director of a carrier of the issue or revocation of certain telecommunications interception warrants, rather than a 'chief officer' as currently allowed for under the TIA Act. This is to provide 'greater operational flexibility for agencies, whilst still maintaining an appropriate level of accountability' (**items 32, 34, 39-40**)[19]
- adding some additional notification requirements for service-based named person warrants and device-based named person warrants, requiring that the chief officer of an agency must notify the Secretary of the Attorney-General's department of any such warrants, and if any additions are then proposed to be added to that warrant, a description 'sufficient to identify the services or devices to be added to the warrant' (**item 31, proposed section 59A**).

17. Explanatory Memorandum, Telecommunications (Interception) Bill 2006, at: http://parlinfoweb.parl.net/parlinfo/Repository/Legis/oldEms/Linked/16050612.pdf.
18. Explanatory Memorandum, p. 5 and p. 8.
19. Explanatory Memorandum, p. 8.

Concluding comments

The Minister has flagged that because of the impending sunset date of 13 June 2008 for the existing 'network protection provisions' in the TIA Act, the government would like the Parliament to consider this a time-critical bill.[20] While the extension of the sunset clauses and the technical amendments contain no new powers for security or law enforcement agencies, the extension of the 'network protection provisions' for a further 18 months continues to allow network protection officers, or those responsible for 'professional standards', of more than 20 Commonwealth and state law enforcement and security agencies access to telecommunications without a warrant or any legislated authorisation process.

New legislation addressing the need for law enforcement and security agencies to protect their networks, which the Attorney-General says will impact on government, corporate and private networks and will involve complex privacy issues and state and territory laws,[21] will presumably be introduced well before the new sunset date of 12 December 2009.

20. Hon. Robert McClelland MP, op. cit.

21. ibid.

Members, Senators and Parliamentary staff can obtain further information from the Parliamentary Library on (02) 6277 2434.