Parliament of Australia
Department of Parliamentary Services

Parliamentary Library
Information, analysis and advice for the Parliament

BILLS DIGEST

www.aph.gov.au/library

26 October 2009, no. 47, 2009–10, ISSN 1328-8091

Telecommunications (Interception and Access) Amendment Bill 2009

Mary Anne Neilsen
Law and Bills Digest Section

Contents

Telecommunications (Interception and Access) Amendment Bill 2009

Date introduced: 16 September 2009

House: House of Representatives

Portfolio: Attorney-General

Commencement: The day 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

The Bill amends the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to introduce a new network protection regime to cover all Australian computer network owners and operators.

Background

Network protection and the current regime

Network protection usually involves establishing perimeters to defend a network by placing protective tools at different points within the network to detect and respond to known and predicted security risks.[1] Such activities are critical to both the network's efficient operation and the protection of all data stored on the network. Such data may include sensitive government and business data held on the network, as well as any personal and financial data which individuals have supplied, for example in the course of their employment or in requesting or purchasing services.[2]

1. Attorney-General's Department, *Discussion paper and exposure draft legislation: computer network protection*, AGD, Canberra, July 2009, p. 1.
2. Ibid.

Under the TIA Act, it is prohibited to intercept, or authorise interception, of a communication passing over[3] a telecommunications system, and to access stored communications, except in accordance with a telecommunications warrant.[4]

However an exemption is provided under section 5F to these prohibitions 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.[5] 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. These exemptions authorise these employees, who are the network administrators of the agencies concerned, to access telecommunications passing over the agencies' networks, without warrant, for the purposes of network security and enforcement of professional integrity.[6]

These exemptions, known as the 'network protection provisions' were inserted by the *Telecommunications (Interception) Amendment Act 2006* and initially only applied to the Australian Federal Police, although the 2007 amending Act[7] extended this to cover designated Commonwealth agencies, security authorities and eligible state authorities.[8] The provisions originally had a two year sunset clause, which was then extended to December 2009. The intention of this delayed sunset clause was to enable law enforcement and security agencies to continue to protect their networks while a comprehensive long-term solution covering both the public and private sectors was developed.[9]

In July 2009, the Government released a discussion paper and exposure draft Bill aimed at providing the solution to network protection for all computer networks. In the short

---

3. A communication is taken to start passing over a telecommunication system when is sent or transmitted, and is taken to continue to 'pass over' the system until it becomes accessible to its intended recipient.

4. Sections 7 and 108 of the TIA Act.

5. Senate Standing Committee on Legal and Constitutional Affairs, *Telecommunications (Interception and Access) Amendment Bill 2008*, May 2008, p. 4.

6. Ibid.

7. *Telecommunications (Interception and Access) Amendment Act 2007.*

8. The Bills Digest for the 2007 Bill describes these agencies in more detail. Under the current arrangements over 20 Commonwealth and state/territory law enforcement and security agencies have exemptions until December 2009. *Telecommunications (Interception and Access) Amendment Bill 2007*, Bills digest, no. 10, 2007–08, Parliamentary Library, Canberra, 2007, p. 8.

9. R. McClelland, 'Second Reading Speech: Telecommunications (Interception and Access) Amendment Bill 2008', House of Representatives, *Debates*, 20 February 2008, p. 5.

consultation period for this draft, the Attorney-General's Department received 19 substantive submissions, although these were not publicly released.[10] Electronic Frontiers Australia (EFA)[11] publicly opposed this draft Bill, pointing out that it did not 'provide sufficient clarity or adequate protections for the privacy of network users'. EFA stated that the 'exposure draft allowed a very broad discretion to network operators to intercept communications' and that the wording of that Bill 'would have permitted network operators to intercept communications, for example, to determine whether peer-to-peer filesharing traffic was infringing a third party's copyright interest, or to determine whether the network was being used for excessive personal use'.[12] It would also have provided a broad ability for network operators to disclose the substance of intercepted communications to an unlimited group of people for undefined 'disciplinary purposes'.[13]

The Minister's Second Reading Speech to the Bill notes that the exposure draft Bill has been modified to address a number of concerns raised in submissions in order to strike an effective balance between protecting networks from malicious activities while protecting users from unnecessary or unwarranted intrusion.[14]

Committee consideration

The Bill has been referred to the Senate Legal and Constitutional Affairs Committee for inquiry and report by 16 November 2009. Details of the inquiry are at:

http://www.aph.gov.au/senate/committee/legcon_ctte/telecommunications/index.htm

The Digest draws on submissions to the inquiry.

Position of significant interest groups/press commentary

Electronic Frontiers Australia (EFA) in their submission to the Senate inquiry, notes that the Bill addresses all of the concerns they raised on the exposure draft.[15] The

10. Attorney-General's Department, *Submission to Senate Standing Committee on Legal and Constitutional Affairs: Telecommunications (Interception and Access) Amendment Bill 2009*, October 2009.

11. EFA is a not-profit national organisation representing internet users concerned with online freedoms and rights.

12. Electronic Frontiers Australia, *Submission to Senate Standing Committee on Legal and Constitutional Affairs: Telecommunications (Interception and Access) Amendment Bill 2009*, October 2009. The submission sets out the problems with the exposure draft but notes also that the current Bill addresses all of the EFA's concerns.

13. Ibid.

14. R. McClelland, 'Second Reading Speech: Telecommunications (Interception and Access) Amendment Bill 2009', House of Representatives, *Debates*, 16 September 2009, p. 9708.

15. See above for further detail.

submission commends the Attorney-General's Department on achieving a workable legislation exception to the prohibition on interception of telecommunications that allows network operators to perform legitimate network protection duties without unduly burdening the privacy of end users.[16]

The Office of the Privacy Commissioner (OPC) recognises the need for an appropriate balance between the public interest in computer network owners and operators being able to undertake legitimate activities aimed at detecting and responding to security risks and maintaining individual privacy. Their submission suggests a number of amendments to improve this balance. For example they suggest tightening the provisions dealing with secondary uses of information and recommend that consideration be given to including in the Bill a provision to allow individuals access to intercepted communications, that relate to them, to be modelled on National Privacy Principle 6.1 in the *Privacy Act 1988*.[17]

The Internet Industry Association is reportedly pleased with the Bill and the changes made since the exposure draft. Their spokesman, John Hilvert, has been reported as saying that the exposure draft might have given internet service providers a new discretionary ability that conflicted with their obligations under privacy laws and the TIA Act generally.[18]

Specific concerns of these and other organisations are referred to in the main provisions section below.

Financial implications

The Explanatory Memorandum states that the Bill will have no financial impact.[19]

16. Electronic Frontiers Australia, op. cit.
17. Office of the Privacy Commissioner, *Submission to Senate Standing Committee on Legal and Constitutional Affairs: Telecommunications (Interception and Access) Amendment Bill 2009*, October 2009.
18. K. Dearne, 'ISPs force cybercrime law rewrite', *Australian*, 29 September 2009, p. 33.
19. Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2009, p. 2 (hereon referred to as the Explanatory Memorandum).

Main provisions

Schedule 1— Amendments to the TIA Act—Network protection

Repeal of existing network protection provisions

The *Telecommunications (Interception) Amendment Act 2006* inserted the existing network protection provisions into sections 5F and 5G of the TIA Act. These provisions are limited to Commonwealth law enforcement agencies and security authorities, and eligible authorities of a State. They are subject to a sunset clause and are due to expire at the end of 12 December 2009.[20] **Items 5 – 8** repeal these provisions as they are to be replaced with the new network protection regime as set out in the Schedule.

Definitions

Items 1 to 4 and **9** provide key definitions underlying the new network protection provisions. They are discussed below in their relevant context.

Interception for network protection duties

Item 11 amends subsection 7(2) by inserting **proposed paragraph 7(2)(aaa)**. It is the central provision of the Bill and creates an exception to the prohibition on the interception of communications by persons lawfully engaged in *network protection duties* in relation to a computer network where that interception is reasonably necessary for the person to effectively perform their duties.

'Network protection duties' are defined in **item 2** as relating to:

- the operation, protection or maintenance of the network, or
- if the computer network is operated by, or on behalf of, a designated Commonwealth agency, security authority or eligible authority of a State,
  - ensuring that the network is *appropriately used* by employees, office holders or contractors of the agency or authority.

'Appropriately used' in this context is defined as:

- when the employee, office holder or contractor have made a written undertaking to comply with any conditions specified by the agency or authority,
- those conditions are reasonable, and
- the person complies with those conditions when using the network (**proposed section 6AAA, item 9**).

20. Explanatory Memorandum, p. 6.

In contrast to the exposure draft, the Bill now limits 'network protection duties' for all networks to duties relating to 'the operation, protection or maintenance of the network'. The ability to intercept communications in order to determine whether a network is being appropriately used is expressly limited to operate only in relation to users of certain Commonwealth agencies, security authorities, or eligible State authorities.

The Explanatory Memorandum states that allowing specified government agencies and authorities to undertake network protection activities for disciplinary purposes is consistent with the existing network protection provisions. These agencies are subject to additional statutory requirements not applicable to other public sector or non-government employers which prescribe particular information handling obligations. The Explanatory Memorandum also states:

> The requirement to act in accordance with reasonable conditions set out in a written user agreement is new and will provide additional protection to workers in the agencies and authorities covered by these provisions.[21]

Interception of speech for network protection purposes

Paragraph 7(2)(aaa) does not allow the interception of speech for network protection purposes (**proposed subsection 7(3), item 13**). The Explanatory Memorandum explains that data relating to Voice over Internet Protocol (VoIP) speech 'may be interrogated but the data cannot be reconstructed in order to listen to the actual voice communication'. The rationale given is that this limitation is intended to preserve the integrity of the interception warrant regime by excluding telephone conversations and communications from the exception so that normal voice communications cannot be listened to.[22]

EFA note that this limitation does not prevent recorded voice communications embedded in video or audio files such as music videos or audio files downloaded from the internet that may be attached to an email communication from being intercepted, reconstituted and listened to for the purposes of paragraph 7(2)(aaa).

EFA argues that it is not clear why the prohibition on assembling voice data should apply only to some voice communication and not to recorded voice communications embedded in video or audio files. In the absence of a good reason, EFA therefore recommends that the prohibition on reconstructing voice communications should be extended to all audiovisual communications.[23]

---

21. Explanatory Memorandum, p. 8.
22. Explanatory Memorandum, p. 10.
23. Electronic Frontiers Australia, op. cit.

Use and disclosure of intercepted communications by authorised persons

Item 15 inserts **proposed sections 63C, 63D** and **63E** which are the main provisions relating to the use and disclosure of intercepted communications by authorised persons under new paragraph 7(2)(aaa).

Proposed section 63C provides that a person engaged in *network protection duties* may, in performing those duties, use or disclose lawfully intercepted communications whether originating internally or externally. The lawfully intercepted communication may be disclosed to either the *responsible person*[24] for the network or to another person if it is reasonably necessary to enable the other person to perform their duties in relation to protecting the network.

Proposed section 63D deals with the use of intercepted information for disciplinary purposes. It allows a person engaged in network protection duties to disclose this information to another person in order to determine:

- if disciplinary action should be taken in relation to the use of the network by an employee, office holder or contractor of a designated Commonwealth agency, security authority or eligible State authority who has legitimate access to the network,
- taking disciplinary action in relation to the use of the network by such an employee, office holder or contractor when the use of the network is not appropriate,[25] or
- reviewing a decision to take such disciplinary action.

Proposed subsection 63D(4) prevents a person from communicating or making use of information accessed under new paragraph 7(2)(aaa) relating to disciplinary action if to do so would contravene another law of the Commonwealth, State or Territory. The Explanatory Memorandum explains the purpose of this provision as providing protection for workers by ensuring that their employer cannot circumvent any relevant workplace relations requirements or workplace surveillance laws by accessing information under the TIA Act.[26]

---

24. The 'responsible person' is defined broadly in **item 4**. It could be the owner of the computer network or the individual operating the network on behalf of the owner. In the case of a body, including a body corporate, the responsible person could be the head of the body who owns or controls the computer network or on whose behalf the computer network is operated, or a person acting as that head, or a person holding (or acting in) a position nominated by the head (or the acting head) of that body. The Explanatory Memorandum at page 6 gives examples.
25. 'Appropriate use' of the network is defined in item 9, see above at p. 6.
26. Explanatory Memorandum, p. 12.

The OPC submission raises a concern with section 63D noting that it could be lawful for a network owner or operator to use and disclose an intercepted communication for disciplinary action even though that use of the network does not pose a network security risk.[27] OPC recommends that the Bill should clarify that disciplinary action in section 63D, regarding misuse of the computer network, applies to activities that pose a risk to network security only.[28]

Proposed section 63E allows a responsible person for a computer network to voluntarily communicate lawfully intercepted information, other than foreign intelligence information, to an officer of an agency in certain circumstances. The responsible person may only communicate the information if he or she suspects, on reasonable grounds, that the information is relevant to determining whether another person has committed a prescribed offence. A prescribed offence is defined in subsection 5(1) and is generally an offence punishable by imprisonment for a maximum period of at least three years.

In effect, this provision allows for a person to voluntarily disclose to a law enforcement agency information which has been intercepted in the course of undertaking network protection duties. The Explanatory Memorandum further explains that lawfully intercepted information may be communicated to an agency regardless of whether it was collected in accordance with a user agreement.[29]

The Law Council of Australia, while not objecting in principle to this provision, would be concerned if law enforcement agencies were to use this voluntary disclosure provision to obtain information by request, when they would otherwise require a warrant to access it.[30]

While acknowledging that the Explanatory Memorandum clarifies that an agency may not compel or request the disclosure of information obtained through network protection duties, the Law Council is concerned that that an agency is not expressly prohibited or prevented from requesting the disclosure of information.

The Law Council submits that a further subsection be added to proposed section 63E which provides that the section does not apply where an agency has requested the

27. Office of the Privacy Commissioner, op. cit, p. 5. The submission gives the example of an IT policy that may regulate an individual's use of the computer network for non-work related purposes such as internet banking.

28. Ibid.

29. Explanatory Memorandum, p. 12.

30. Law Council of Australia, *Submission to Senate Standing Committee on Legal and Constitutional Affairs: Telecommunications (Interception and Access) Amendment Bill 2009*, October 2009.

disclosure of the information. This would safeguard against the potential misuse of the section to circumvent the warrant requirements of the Act.[31]

Item 22 inserts **proposed section 79A** which provides the rules regarding the destruction of a 'restricted record', that is, a record of a communication that was intercepted under paragraph 7(2)(aaa). A responsible person for a computer network must ensure the record be destroyed as soon as practicable after it is determined that it is not likely to be required for network security purposes or disciplinary action.

Several submissions to the Senate inquiry commented on this provision.

The Australian Law Reform Commission and the OPC submissions note that section 79A extends only to the destruction of the original record and that there should also be an obligation to destroy copies of restricted records.[32] The Explanatory Memorandum notes that this is not practical as often copies of records are no longer in the possession of the responsible person.[33]

EFA also notes that it is not clear what the requirements are for the destruction of such records. For example 'destroy', in this situation, could mean merely 'delete' where the data remains on the storage media but the index providing its location is removed. EFA submits that the requirement to destroy intercepted communication should explicitly reference acceptable standards of secure electronic document destruction as appropriate to the sensitive nature of intercepted communications.[34]

EFA also suggested a further tightening of the wording in section 79A, noting that the requirement to destroy records only applies 'as soon as practicable after [a relevant person becomes] satisfied that the restricted record is not likely to be required' for network protection duties or for disciplinary action purposes. EFA argues that the prospective nature of this phrasing suggests that there is no requirement to destroy a record of an intercepted communication once the legitimate purpose for which it was intercepted has been fulfilled. EFA submits that proposed subsection 79A(2) be amended to additionally require destruction of applicable records as soon as practicable after the relevant person becomes satisfied that the record is no longer likely to be required.

Item 21 is a consequential amendment flowing from **item 22**. It clarifies that the destruction of records requirements in new section 79A (as opposed to those in existing

31. Ibid. The submission states that this would be in line with the voluntary disclosure provisions (sections 174 and 177) which are similar in effect to proposed section 63E.

32. Australian Law Reform Commission, *Submission to Senate Standing Committee on Legal and Constitutional Affairs: Telecommunications (Interception and Access) Amendment Bill 2009*, October 2009, pp 2–3, Office of the Privacy Commissioner, op. cit p. 2.

33. Explanatory Memorandum, p. 14.

34. Electronic Frontiers Australia, op. cit.

section 79) will apply to records intercepted for network protection under new paragraph 7(2)(aaa). The Explanatory Memorandum explains the rationale for having two different provisions dealing with destructions of records.[35]

Schedule 2—Other amendments to the TIA Act

Schedule 2 makes amendments to the TIA Act mainly relating to the definition of 'permitted purpose' and to the evidential certificate regime.

'Permitted purpose'

Item 2 would amend the definition of 'permitted purpose' in subsection 5(1). Section 67 of the TIA Act allows information which has been lawfully intercepted to be used for certain defined permitted purposes, including a purpose connected with an investigation by the AFP of a prescribed offence.[36] **Item 2** inserts **new subparagraphs (5)(1)(b)(v)** and **(vi)**, the effect being that lawfully intercepted information could be used, communicated, and used in proceedings by the AFP in applications for control orders and preventative detention orders under Divisions 104 and 105 of the *Criminal Code Act 1995*.[37] The Explanatory Memorandum states that this is not a new police power but a clarification of an existing power.[38]

Items 3 and **4** propose further amendments to the definition of 'permitted purpose' in order to reflect changes to the powers of the New South Wales Police Integrity Commission (PIC) made under the *Police Integrity Act 1996* (NSW). In the case of **item 4**, the effect will be to enable the PIC to use and communicate lawfully intercepted information for the purpose of an investigation in relation to any officer within the PIC's jurisdiction.

Evidentiary certificates

Items 9 to **13** propose several amendments regarding the use of evidentiary certificates. Under the TIA Act an evidentiary certificate may be used in certain circumstances. Such a certificate may be received in evidence in a proceeding without further proof and is conclusive evidence of the matters stated in the documents.[39]

---

35. Ibid.
36. A prescribed offence is defined in subsection 5(1) and is generally an offence punishable by imprisonment for a maximum period of at least three years.
37. Divisions 104 and 105 were introduced in 2005 in relation to the prevention of terrorist acts.
38. Explanatory Memorandum, p. 24.
39. Subsection 18(2) of the TIA Act.

Item 9 would repeal and replace **subsection 18(1)**. Section 18 deals with evidentiary certificates that may be issued by the Managing Director or the Secretary of a telecommunications carrier in relation to the issuing of ASIO interception warrants. The **new subsection 18(1)** would have the effect of allowing the Managing Director or the Secretary to delegate this power by authorising employees of the carrier to also issue certificates. The Explanatory Memorandum notes that the delegation of this power is consistent with the current evidentiary certificate regime applying to law enforcement interception warrants under section 61 of the TIA Act.[40]

Item 11 would repeal and replace **subsection 129(1)** and is similar in effect to item 9. It would allow the Managing Director or the Secretary of a carrier to delegate to employees the power to issue evidentiary certificates in relation to stored communication warrants.

Chapter 4 of the TIA Act allows access to telecommunications data obtained under an authorisation. **Item 13** inserts **proposed sections 185A, 185B** and **185C** into this Chapter. The effect would be to extend the evidentiary certificate regime to lawful access to telecommunications data authorised under this Chapter. The provisions are modelled on existing evidentiary certificate provisions contained in other Chapters and include the powers of delegation mentioned above in items 9 and 11.

Concluding comments

Generally the Bill has been well received. It is seen as an improvement on the initial exposure draft produced earlier this year in providing a better balance between the needs of internet security and the protection of personal privacy. The Office of the Privacy Commissioner and Electronic Frontiers Australia have however made recommendations aimed at tightening the use and disclosure provisions of the proposed regime.

The Senate inquiry into the Bill is due to report on 16 November 2009 and the current arrangements for network protection expire on 12 December 2009. Parliament therefore has a short time frame in which to consider the Bill and the Report.

40. Ibid., p. 19.

Members, Senators and Parliamentary staff can obtain further information from the Parliamentary Library on (02) 6277 2438.