CHAPTER 2

OVERVIEW OF THE BILL

2.1 The primary 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 makes it an offence to intercept communications or to access stored communications, other than in accordance with the provisions of the Act. The… TIA Act [also] specif[ies] the circumstances in which it is lawful to intercept, access communications or authorise the disclosure of telecommunications data.[1]

2.2 The Bill seeks to amend the TIA Act to ensure that network operators can undertake legitimate activities aimed at securing the integrity of their network and the information it contains.[2]

Legitimate network protection activities

2.3 In recent times, the use of online services by individuals, governments, businesses and the not-for-profit sector to store and transmit sensitive information has increased. Protecting information and computer infrastructure from disruption or malicious access by criminal elements seeking to gain a financial or other benefit is therefore a growing priority for governments and computer network owners.[3]

2.4 Network owners and operators typically use automated network protection systems to screen and reject incoming communications if it is suspected that they contain 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.[4]

2.5 While the use of gateway control systems (such as virus protection software) does not generally violate interception legislation, network owners and operators

---

1 *Telecommunications (Interception and Access Act 1979*, Annual Report for the year ending 30 June 2008, p. 2.

2 The Hon Robert McClelland MP, Attorney-General, Second Reading Speech: Telecommunications (Interception and Access) Amendment Bill 2009, *House of Representatives Hansard*, 16 September 2009, p. 9708.

3 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 1.

4 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2008*, p. 3.

undertaking network protection activities at the threshold of a network are vulnerable to inadvertent technical breaches of the TIA Act.[5]

> Whether an activity is lawful depends on the particular characteristics of the activity that is undertaken, where it is undertaken, by whom, and whether or not there is awareness by the affected person that it is being done. For example, persons undertaking network protection activities may need to copy a communication before it is delivered to the intended recipient. However, under the TIA Act, copying is only allowed at certain points in the delivery of that communication and under certain conditions.[6]

2.6 The main interception prohibitions contained in the TIA Act are found in sections 7 and 108. These sections prohibit interception of telecommunications that are passing over a telecommunications system and access to stored communications, except in accordance with a telecommunications interception warrant.

2.7 The TIA Act also contains special exemptions for security agencies and certain Government departments to allow access to communications on their own computer networks for network protection activities and for the enforcement of professional standards. These 'network protection provisions,'[7] contained in section 5F(2) and 5G(2) of the TIA Act, have the effect of providing a temporary exemption from the section 7 requirements for certain employees with responsibility for network protection or maintenance and allow these government employees to access and/or copy any communication from within or passing over the agencies' network for the enforcement of professional integrity. As the Attorney-General's Department submission explained:

> These provisions were originally introduced by the *Telecommunications (Interception) Amendment Act 2006* in order to allow the Australian Federal Police (AFP) to protect its network and to ensure staff were complying with the AFP's professional standards. At the time, Parliament legislated a two year sunset period for the provisions in order to allow consideration of a more comprehensive solution.
>
> In 2007, the provisions were widened to the current form to allow government agencies and authorities with a security or law enforcement focus to monitor communications for the purpose of protecting their networks and enforcing professional standards without the risk of breaching the TIA Act.[8]

---

5 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2008*, p. 3.

6 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 1.

7 The Hon Robert McClelland MP, Attorney-General, Second Reading Speech: Telecommunications (Interception and Access) Amendment Bill 2008, *House of Representatives Hansard*, 20 February 2008, p. 836.

8 Attorney-General's Department, *Submission 3*, p. 2.

2.8 In May 2008 the committee reported on an inquiry into the *Telecommunications (Interception and Access) Amendment Act 2008*. The main purpose of that Bill was to extend sunset provisions that apply to the network protection provision to allow sufficient time for the development of a comprehensive solution covering both the public and private sectors.[9] At that time, the Committee recommended that:

> …if further legislation proposing amendments to the network protection provisions (including to sunset clauses) is introduced, such legislation should include a thorough and considered response to achieving a balance between individual privacy rights and network protection requirements. Such a review should assess mechanisms to mitigate intrusiveness and abuse of access, and consider how secondary data may be managed appropriately.[10]

2.9 According to the Explanatory Memorandum, this Bill amends the TIA Act:

> …to implement a full legislative solution that clarifies the basis on which communications can be accessed for the purposes of protecting a computer network.[11]

Existing Arrangements

2.10 As stated above, the primary objective of the TIA Act is to protect the privacy of individuals who use the Australian telecommunications system.[12] One way the TIA achieves this is by prohibiting the interception of a communication that is 'passing over' a telecommunications system.[13]

2.11 Existing section 5F defines when a communication is considered to be 'passing over' a telecommunications system. Broadly, a communication is taken to start passing over a telecommunication system when it is sent or transmitted by the sending person – paragraph 5F(1)(a) – and is taken to continue to pass over the system until it becomes accessible to the intended recipient – paragraph 5F(1)(b). For example, an email is taken to start passing over a telecommunications system when the email is sent and is taken to finish passing over that system when it becomes accessible to the intended recipient (i.e. it 'arrives' in the recipient's email inbox).

---

9 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 1.

10 Senate Standing Committee on Legal and Constitutional Affairs, *Report into the Telecommunications (Interception and Access) Amendment Bill 2008*, May 2008, p. 17.

11 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 1.

12 *Telecommunications (Interception and Access) Act 1979*, Annual Report for the year ending 30 June 2008, p. 2.

13 Subsection 7(1), *Telecommunications (Interception and Access) Act 1979.*

2.12 Existing subsection 5F(2) alters that definition by stating that, if the communication is sent from an address on a computer network operated by a Commonwealth agency, security agency or eligible authority of a state, it is not taken to have started passing over the telecommunication system until it is no longer under the control of certain employees (i.e. those responsible for managing the agency's network or those responsible for the enforcement of professional standards in the agency).

2.13 Defining when a communication is passing over a telecommunication system in this way has the effect of enabling:

> …communications which are within the network boundaries of the relevant agency or authority's network to be copied or recorded in order to allow *network protection duties* concerning the operation, protection or maintenance of the network, or upholding professional standards, to be performed by personnel within those bodies other than the sender.[14]

2.14 Existing section 5G similarly modifies the definition of the 'intended recipient' to allow certain communications within Commonwealth agencies, security authorities and eligible authorities of a State to be copied or recorded. Subsection 5G(2) outlines that such interception may only be conducted:

> …in order to allow duties concerning the operation, protection or maintenance of the network, or upholding professional standards, to be performed by personnel within those bodies other than the addressee.[15]

2.15 Both subsections 5F(2) and 5G(2) are the subject of sunset clauses (contained in subsections 5F(3) and 5G(3) respectively) meaning they cease to have effect at the end of 12 December 2009. After this date, employees of Commonwealth agencies, security authorities and eligible authorities of a State with network protection responsibilities would require a warrant to copy or record communications, even in the course of their network protection duties.

The Proposed Arrangements

2.16 The Bill seeks to establish a permanent regime that will:

- enable all owners and operators of computer networks to undertake activities to operate, maintain and protect their networks;
- enable Commonwealth agencies, security authorities and eligible State authorities to ensure that their computer network is appropriately used by employees, office holders or contractors of the agency or authority;

---

14 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 6.

15 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 6.

- limit secondary use and disclosure of information obtained through network protection activities to:
  - network protection purposes;
  - undertaking disciplinary action against an employee, office holder or contractor of a Commonwealth agency, security authority and eligible authority of a State who has been given access to a network; and
  - reporting illegal behaviour that attracts a minimum of three years' imprisonment penalty threshold to the relevant authorities; and
- require the destruction of records obtained by undertaking network protection activities when the information is no longer required for those purposes.

Interceptions for Network Protection Purposes

2.17 The Bill (at Items 5-8), by repealing subsections 5F(2), (3) and 5G(2), (3) and (4), seeks to simplify the definition of when a communication is passing over a telecommunication system (and the definition of 'intended recipient') so that the definition applies generically, regardless of whether the communication is sent from within a government agency or not.

2.18 Item 11 of the Bill then inserts paragraph 7(2)(aaa), which lifts the prohibition on the interception of a communication by a person (contained in subsection 7(1)) if the person is appropriately authorised to engage in network protection duties and it is necessary for the person to intercept the communication in order to perform those duties effectively.

2.19 Importantly, the proposed regime would allow certain authorised people in both government and non-government agencies to intercept non-voice communications for network protection purposes.[16] That is, the regime contained in the Bill would not be limited in application to employees of Commonwealth agencies, security authorities and eligible authorities of a State (though it would apply in these agencies). Furthermore, this exception would not be subject to a sunset clause.

2.20 Item 13 of the Bill inserts a paragraph which ensures that the prohibition contained in subsection 7(1) still applies to a voice communication in the form of speech (including a communication that involves a recorded or synthetic voice).

2.21 As the Explanatory Memorandum explains:

> In the case of Voice over Internet Protocol (VoIP), the voice communication in the form of packet data may be intercepted and

16 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 8.

> interrogated but the data may not be reconstructed in order to listen to the actual voice communication.
>
> 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.
>
> Recorded voice communications embedded in video or audio files such as a music video or audio file downloaded from the internet that may be attached to an email communication can be intercepted, reconstituted and listened to for the purposes of communicating or making use of communications intercepted under new paragraph 7(2)(aaa).[17]

'Appropriate use' of Government Networks

2.22 The Bill allows network owners and operators from both the private and public sectors to intercept communications in certain circumstances, particularly where that interception is necessary for network protection purposes. Only Government network operators, however, will be able to intercept communications to ensure that staff use the network appropriately.

2.23 Item 9 of the Bill inserts new section 6AAA. Section 6AAA defines when a network is 'appropriately used' by an employee, office holder or contractor of a Commonwealth agency, security agency or eligible authority of a State. An employee's use of the network is considered appropriate when they have undertaken (in writing) to use the network in accordance with reasonable (written) conditions specified by the agency and where their use is in compliance with those conditions.

2.24 This definition of 'appropriate use' is designed to be flexible enough to recognise that what constitutes appropriate use of a computer network may vary between agencies.[18]

2.25 While user agreements must be reasonable and must comply with all relevant Commonwealth, State and Territory laws,

> …[t]he Bill does not require a new user agreement to be entered into. Existing user agreements will suffice where an employee, office holder or contractor of an agency or authority has undertaken to comply with the conditions set out in the agreement and those conditions are reasonable.[19]

---

17 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 10.

18 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 7.

19 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 7.

2.26 Furthermore, the absence of an agreement does not preclude an agency or authority from recording information transiting their network for duties relating to the operation, protection or maintenance of the network.

> However, an agency or authority will not be able to record information transiting their network to ensure the network is appropriately used, nor secondarily use or disclose information accessed for disciplinary purposes. This is because new subsection 63D(2) at Item 15 only authorises disciplinary action to be taken in relation to 'appropriate use' of the network, not 'use' of the network.[20]

Secondary use and disclosure

2.27 The Bill also limits the use and disclosure of information obtained through network protection activities to activities relating to the protection of the network, the reporting of illegal behaviour (where that behaviour attracts a minimum penalty of three years' imprisonment) to the relevant authority, and to undertaking disciplinary action against an employee, office holder or contractor of a Commonwealth agency, security authority and eligible authority of a State who has been given access to a network.

Network Protection

2.28 Item 15 of the Bill also inserts new sections 63C which sets out the terms under which a person engaged in network protection duties may communicate or make use of the information they intercept.

2.29 Subsection 63C(1) and (2) allow a person engaged in network protection duties to disclose that information which has been lawfully intercepted in the course of their duties or to disclose that information to another person with network protection duties if it is reasonably necessary to enable the other person to perform their duties. These subsections are limited by new subsection 63C(3) which does not allow the use or disclosure of a communication that has been converted into a voice communication in the form of speech.

2.30 Items 17-20 of the Bill:

> …ensure that the limitations on the use and disclosure of information related to disciplinary action will apply to further use and disclosures regardless of the number of times the information is used or disclosed. These amendments will also ensure that a person who receives information related to disciplinary action under subsection 63D(2), may only communicate, use or record that information where doing so does not contravene another law of the Commonwealth or a State or Territory.[21]

---

20 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 7.

21 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, pp. 12-13.

Disciplinary purposes

2.31 Item 15 of the Bill inserts new section 63D, allowing a person engaged in network protection duties to disclose (lawfully) intercepted information to another person in order to determine whether disciplinary action should be taken. This provision limits this on-disclosure to determinations about the appropriate use of a network by an employee who is an employee or office holder (or contractor) of a Commonwealth agency, security authority or eligible State authority and who has legitimate access to that network.[22]

Destruction of records

2.32 A 'restricted record' is defined in subsection 5(1) of the TIA Act as 'a record other than a copy that was obtained by means of an interception, whether or not in contravention of subsection 7(1), of a communication passing over a telecommunications system.'[23]

2.33 Current section 79 of the TIA Act sets out that where a 'restricted record is not likely to be required for a permitted purpose in relation to the agency, the chief officer must cause the restricted record to be destroyed. These requirements only currently apply to interception agencies. As stated in the Explanatory Memorandum, the new provisions:

> …when combined with the new destruction requirements under new section 79A at Item 22 would create a different regime for interception agencies. [Requiring the same regime] would impose an onerous administrative burden on agencies as the destruction requirements in section 79 are imposed on an agency's chief officer. In practice this would mean that the chief officer of an agency would need to destroy every record of a network protection activity when it is no longer needed. In some agencies this could amount to thousands of records at any point in time.[24]

2.34 The Bill seeks to address this by inserting new subsection 79(3) which ensures that new section 79A will apply to any records intercepted for network protection duties (under new paragraph 7(2)(aaa)) while section 79 would only apply to interception agencies.

2.35 Records of a communication intercepted under proposed paragraph 7(2)(aaa) must be destroyed once the responsible person (that is, the individual or head of the body which operates the network) is satisfied that the record is not likely to be required for network protection duties.

---

22 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 11.

23 *Telecommunications (Interceptions and Access) Act 1979*, subsection 5(1), definition of 'restricted record'.

24 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 13.

2.36 Where the network is operated by a Commonwealth agency, security authority or eligible authority of a State and the communication was intercepted for the purpose of determining whether disciplinary action should be taken (or taking that action), the responsible person must cause that record to be destroyed as soon as practicable after becoming satisfied that the record is not likely to be required.[25]

Definition of 'permitted purpose'

2.37 Schedule 2 of the Bill contains a number of provisions which amend or supplement the definition of 'permitted purpose'. Many of these amendments clarify current practices or alter the definition to reflect changes in other acts.

2.38 Item 2 inserts new subparagraph 5(1)(b)(v), which clarifies that lawfully intercepted information can be communicated in seeking or issuing a control order pursuant to Division 104 of the *Criminal Code*. Currently, section 67 of the TIA Act allows lawfully intercepted information to be used for a 'permitted purpose', which includes a purpose connected with an investigation by the AFP of a prescribed offence (defined). This amendment clarifies the TIA Act to avoid doubt that the AFP may use and communicate lawfully intercepted information when seeking the Attorney-General's approval, to apply for an interim control order, or when applying for the control order to the courts. New subparagraph (b)(vi), which is also inserted by this item, clarifies that lawfully intercepted information can also be used or communicated in relation to preventative detention orders sought and issued pursuant to Division 105 of the *Criminal Code*.[26]

2.39 According to the Explanatory Memorandum:

> The amendments to *permitted purpose* in relation to the use or disclosure of information related to Divisions 104 and 105 of the *Criminal Code* are designed to clarify the operation of the existing legislation, rather than expanding police powers.[27]

2.40 Item 14, contained in Part 2 of Schedule 2 of the Bill is designed to ensure that AFP officers who have, in good faith, used or communicated lawfully intercepted information for a purpose connected with Divisions 104 and 105 of the *Criminal Code*, are not liable for any breach of the TIA Act caused by that use or communication.[28]

---

25 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 13.

26 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, pp. 15-16.

27 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 24.

28 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 24.

2.41 Items 3 and 4 of Schedule 2 amend the 'permitted purpose' definition to reflect changes to the *Police Integrity Commission Act 1996* (NSW). This includes amendments to facilitate the transfer of particular functions from the Independent Commission Against Corruption to the Police Integrity Commission. The amendments also ensure that further changes to that Act will be recognised by the TIA Act without the need for further amendments to the Commonwealth Act.[29]

Delegation powers for certificate etc

2.42 Section 18 of the TIA Act currently contains an evidentiary certificate regime for intercepted and stored communications. The regime allows the Managing Director or secretary of a carrier (or of a subsidiary of a parent company of a carrier) to issue a written, signed certificate setting out such facts as he or she considers relevant with respect to acts or things done by, or in relation to, employees of the carrier. These certificates set out facts in relation to a warrant issued to the Australian Security and Intelligence Organisation (ASIO) and include facts that may be relevant in order to have a warrant issued or executed as well as relevant facts pertaining to anything done by an employee of the organisation in connection with the execution of the warrant. These certificates may be received in evidence in exempt proceedings (defined) without further proof and are conclusive evidence of the matters stated in the certificate.

2.43 Items 9-12 of Schedule 2 of the Bill retain this power but allow the Managing Director or secretary to delegate their evidentiary certificate functions by authorising, in writing, an employee of the carrier to issue such a certificate. Although this provision will expand the number of people who can issue evidentiary certificates under section 18 on behalf of a carrier:

> …[e]nabling staff who are more accessible but of sufficient seniority to issue the certificate gives the carrier flexibility, which should ensure that evidentiary certificates can be issued promptly.[30]

2.44 As the Explanatory Memorandum explains:

> …[t]he delegation of this function is consistent with the current evidentiary certificate regime applying to law enforcement interception warrants under section 61 of the TIA Act.[31]

2.45 Item 11 of Schedule 2 makes a similar amendment to section 129, allowing a similar delegation in relation to written evidentiary certificates relating to acts or

---

29 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 16.

30 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 18.

31 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 18.

things done to enable the execution of a stored communications warrant (as opposed to a warrant issued to ASIO).

Telecommunications data to be included in evidentiary certificates regime

2.46 Telecommunications data is information about a communication, other than the content or substance of the communication itself. For example, for a telephone-based communication, telecommunications data would include subscriber information, the telephone numbers of the parties involved, the time of the call and its duration. In relation to internet-based applications, it would include the Internet Protocol (IP) address used for a session and the start and finish time of each session.[32]

2.47 Telecommunications data is available in relation to all forms of communications, including fixed and mobile telephony services and internet based applications, including internet browsing and Voice over Internet Protocol (VoIP).[33]

2.48 Under the current regime, telecommunications data may only be disclosed by a carrier to ASIO in connection with the performance of its functions and to enforcement agencies for the investigation of criminal law, a law imposing a pecuniary penalty or the protection of the public revenue.[34]

2.49 Item 13 of Schedule 2 of the Bill inserts three new sections, 185A, 185B and 185C, which extends the evidentiary certificate regime (discussed above, but also including certificates issued by the Director-General or the Deputy Director-General of Security) to include access to telecommunications data obtained under an authorisation. The new sections apply to historical and prospective telecommunications data and are consistent with the existing evidentiary certificate provisions for interception and stored communications.

---

32 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 20.

33 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 20.

34 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 20.