CHAPTER 2

OVERVIEW OF THE BILL

2.1 The Bill seeks to amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), the primary objective of which 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.[1]

2.2 The TIA Act also recognises that there are legitimate circumstances when it may be necessary to intercept or access telecommunications, such as to facilitate the investigation of serious criminal offences. The second purpose of the Act therefore is to specify the circumstances in which it is lawful to intercept or access telecommunications.

2.3 The amendments in the Bill have three key outcomes, which were the main focus of this inquiry:

- extension of the sunset date for the network protection provisions;
- clarification that a device-based named person warrant gives the authority to intercept multiple telecommunications devices, and that additional devices not identified when the warrant was issued may be added; and
- removal of mandatory requirements for state interception agencies to provide copies of warrants and revocation instruments to state Ministers and for the Ministers to forward these to the Attorney-General's Department.

2.4 The Bill also seeks to make some relatively minor technical amendments.

Extension of sunset clauses for network protection provisions

Introduction

2.5 Sections 7 and 108 of the TIA Act prohibit interception of telecommunications that are 'passing over'[2] a telecommunications system, and access to stored communications, except in accordance with a telecommunications interception warrant.

---

1 *Telecommunications (Interception and Access) Act 1979*, Annual Report for the Year Ending 30 June 2007.

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

2.6 However, an exemption is provided under subsection 5F 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.

2.7 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.

2.8 These exemptions have become known as the 'network protection provisions'[3], and are the subject of the sunset clauses that Items 1 and 2 of Schedule 1 of the Bill seek to amend.

Background on the network protection provisions

2.9 In 2005, the Howard Government appointed Mr Anthony Blunn AO to undertake a review of the regulation of access to communications under the TIA Act. In relation to access for network protection purposes, Mr Blunn found that:

> …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.[4]

2.10 Notwithstanding this, he considered there is a need for the effective protection of agency or enterprise systems from accidental or deliberate damage, such as against unauthorised entry (hacking) and viruses; and for developing and testing new technologies.[5]

2.11 Consequently, Mr Blunn recommended that:

> …subject to appropriate controls, access to communications without warrant be permitted where it is necessarily incidental to the protection of

3 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.

4 A. S. Blunn, AO, *Report of the Review of the Regulation of Access to Communications*, 2005, p. 59.

5 A. S. Blunn, AO, *Report of the Review of the Regulation of Access to Communications*, 2005, pp 57-60.

> data systems or the authorised development or testing of new technologies or interception capabilities.[6]

2.12 The network protection provisions were introduced in a government amendment to the Telecommunications (Interception) Amendment Bill 2006 (the 2006 amendment bill). In their original form, the provisions applied only to the Australian Federal Police (AFP). While the committee conducted an inquiry into the provisions of the 2006 amendment bill, the government amendments were introduced after the committee had concluded its inquiry.[7]

2.13 The passage of the Telecommunications (Interception and Access) Amendment Bill 2007 (the 2007 amendment bill)[8] extended the network protection provisions to cover a broader range of Commonwealth agencies. These included the Australian Commission for Law Enforcement Integrity and the Australian Crime Commission; Commonwealth organisations undertaking roles in relation to security, intelligence, foreign affairs and defence; and eligible state authorities including state police and state integrity and corruption investigation commissions. The sunset clauses were not amended in the 2007 amendment bill.[9]

Summary of provisions

2.14 Items 1 and 2 of Schedule 1 of the Bill will extend the existing sunset provisions in subsections 5F(3) and 5G(3) of the TIA Act until 12 December 2009.

2.15 The Explanatory Memorandum (EM) gives the following explanation for extending the network protection 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.[10]

---

6 A. S. Blunn, AO, *Report of the Review of the Regulation of Access to Communications*, 2005, p. 62.

7 Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006,* March 2006.

8 The amendments in the current Bill relate to only some amendments in the 2006 and 2007 amendment bills which were focussed on other changes to the TIA Act such as stored communications warrants, B-Party (non-suspect) warrants, transferring provisions from the *Telecommunications Act 1997* and implementing other recommendations of the Blunn report.

9 For the Senate Third Reading debate on the 2007 amendment bill, see *Senate Hansard*, 20 September 2007, pp 224-239.

10 EM, p. 3.

Device-based named person warrants

Introduction

2.16 A device-based named person warrant is a form of 'named person warrant'. A 'named person warrant' is 'an interception warrant issued or to be issued under sections 9A, 11B or 46A' of the TIA Act.[11] As explained in the EM to the Bill, named person warrants can relate to either telecommunications services being used by a particular person, or 'a particular telecommunications device' used or likely to be used by the person.[12]

2.17 A 'telecommunication device' is a 'terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system'[13], such as a computer terminal, personal digital assistant or mobile telephone handset. Telecommunications devices can be used to access more than one telecommunications service. For example, it is a simple matter to change the SIM card in a mobile telephone, allowing the phone's user to access more than one telephone service.

2.18 A device-based named person warrant enables an interception agency to lawfully intercept multiple telecommunications *services* accessed with a telecommunications device by a named person. However, the TIA Act currently does not permit agencies to intercept more than one device-based warrant.

Background

2.19 Named person warrants were introduced in 2000.[14] According to the Attorney-General's Department, these warrants were introduced 'to reflect the advances in technology which targets had taken advantage of with the express purpose of avoiding law enforcement detection, such as the use of multiple telecommunications services.'[15]

2.20 Device-based named person warrants were introduced in the 2006 Amendment Bill, with its EM providing the following explanation of their purpose:

> These amendments are designed to assist interception agencies to counter measures undertaken by persons of interest to evade telecommunications interception such as adopting multiple telecommunications services.

---

11 TIA Act, subsection 5(1).

12 EM, p. 4.

13 TIA Act, subsection 5(1).

14 Telecommunications (Interception) Legislation Amendment Act 2000.

15 *Submission* 4, p. 2.

> The amendments will enable interception agencies to apply to an issuing authority for a named person warrant to intercept communications from identified telecommunications devices.[16]

2.21 Device-based named person warrants were intended to be used only when other possibilities have been exhausted, as reflected in the conditions imposed on their use. The EM for the 2006 Bill explained:

> An issuing authority must not authorise interception on the basis of the telecommunications device unless satisfied that the applicant agency has no practicable methods of identifying the telecommunications services used or likely to be used by the person of interest, or that interception of those services would not be possible.[17]

Summary of Provisions

Items 3 to 7 of Schedule 1 of the Bill – security provisions

2.22 Item 3 of Schedule 1 seeks to amend subparagraph 9A(1)(b)(ii) of the TIA Act to clarify that a device-based named person warrant issued under section 9A gives the authority to intercept 'multiple telecommunications devices.' The EM states that this amendment is 'consistent with service-based named person warrants'. The item will replace the words 'a particular telecommunication device' with the words 'telecommunications devices'.[18]

2.23 Items 4, 5, 6 and 7 are described in the EM for the Bill as making 'consequential amendments' to section 9A as a result of Item 3. These items are nonetheless significant.

2.24 Items 4, 5 and 7 will replace the words 'a telecommunications device, identified in the warrant' with the words 'any telecommunications device'. This wording change means that any devices used by the person, including those not identified on the warrant at the time of issue, may be intercepted.

2.25 Item 6 of the Bill will repeal paragraph 9A(2)(ba) of the TIA Act and insert a new paragraph. This paragraph specifies the level of detail that must be included in a device-based warrant sought by the Director-General of Security.

2.26 The existing requirement in the TIA Act is that the warrant 'must include details sufficient to identify the telecommunications device…'. Item 6 will replace these words with the words 'must include details (to the extent that these are known to the Director-General of Security) sufficient to identify the telecommunications devices…', a less stringent identification requirement.

---

16 EM, Telecommunications (Interception) Amendment Bill 2006, p. 34.

17 EM, Telecommunications (Interception) Amendment Bill 2006, p. 34.

18 EM, TIA Amendment Bill 2008, p. 4.

2.27 The amendments proposed in Item 6 are similar to those proposed in Items 11 and 20. They also incorporate the following features which are consistent with the other changes in the Bill in relation to device-based named person warrants:

- multiple devices on a single warrant;
- a less stringent requirement to identify the device or devices; and
- devices do not necessarily have to be identified at the time the warrant is sought, and can be added subsequently.

Items 8 to 12 of Schedule 1 of the Bill– foreign intelligence

2.28 Items 8, 9, 10, 11 and 12 seek to amend section 11B of the TIA Act. The changes proposed in these items are consistent with the overall intent in the Bill of enabling device-based named person warrants to authorise the interception of multiple telecommunications devices. The EM again notes that the changes will make the provisions for device-based named person warrants consistent with those that apply to service-based named person warrants[19].

2.29 Item 8 replaces the words 'a particular' with 'any', reflecting the less stringent requirement to identify the device (as discussed in paragraphs 2.27-2.28 above).

2.30 Items 9 to 12 are described by the EM as making 'consequential amendments…'. Items 9 and 12 replace the words 'a telecommunications device, identified in the warrant' with the words 'any telecommunications device'.

2.31 Item 10 replaces 'a telecommunications device identified in the warrant' with 'any telecommunications device that the person is using, or is likely to use'.

2.32 Item 11 is a similar provision to that described in paragraphs 2.26 - 2.28 above in relation to Item 6. The item replaces the requirement to include 'details sufficient to identify the telecommunications device' with 'details (to the extent that these are known to the Director-General of Security) sufficient to identify the telecommunications devices…'. As is the case for item 6, the item reflects the changes that will authorise multiple devices on a warrant; the less stringent identification requirement; and the addition of devices after the warrant has been issued.

Items 20 to 25 of Schedule 1 of the Bill – law enforcement

2.33 Items 20 to 25 seek to amend Division 3 of Part 2-5 of the TIA Act, specifically sections 42 and 46. Division 3 of the TIA Act allows an agency (for example, the AFP) to apply to an eligible Judge or nominated AAT member for a warrant in respect of a telecommunications service or a person. Warrants authorised under Division 3 are generally for law enforcement purposes.

---

19 EM, p.4.

2.34 Item 20 is similar to those described above in relation to Items 6 and 11. The EM explains that Item 20 amends paragraph 42(4A)(ba) of the TIA Act to allow for multiple telecommunications devices to be included in the affidavit accompanying an interception warrant application[20]. Item 20 will replace the words 'a telecommunications device' with the words 'any telecommunications device'. The item will also replace the words 'details sufficient to identify the telecommunications device…' with the words 'details (to the extent these are known to the chief officer) sufficient to identify the telecommunications devices…'.

2.35 Item 21 replaces the words 'a particular' with 'any'. The EM explains that the amendment will allow for multiple telecommunications devices to be included on an application for a device-based named person warrant[21].

2.36 Items 22 to 25 are described in the EM as amendments consequential to the amendments in Item 21.

Items 13 and 14 of Schedule 1 of the Bill – notification of telecommunications carriers

2.37 Items 13 and 14 of the Bill seek to amend section 16 of the TIA Act. This section requires a 'certifying person' to notify the Managing Director of a carrier when a device is to be added to a device-based named person warrant issued under sections 9A or 11B. These items substitute the words 'a telecommunications device, identified in the warrant' with the words 'any telecommunications device'. The items are described in the EM as amendments consequential to Items 3 and 8.

Item 31 of Schedule 1 of the Bill – Notifications to the Secretary of the Attorney-General's Department

2.38 Item 31 consolidates the requirements for an agency to notify the Secretary of the Attorney-General's Department in relation to lawfully issued telecommunications interception warrants. Significant features of this notification requirement are that the Chief Officer of the intercepting agency must provide to the Secretary of the Attorney-General's Department:

- a copy of every warrant issued to the agency;
- where it is proposed to intercept additional services not identified in a service-based named person warrant, a description in writing sufficient to identify the services to be added to a warrant; and
- where it is proposed to intercept additional devices not identified in a device-based named person warrant, a description in writing sufficient to identify the devices to be added to a warrant.

20 EM, p.6.

21 EM, p.6.

Item 37 of Schedule 1 of the Bill– notification of Managing Directors of carriers

2.39 Item 37 is important as it is one of the key amendments that will, if passed, resolve current inconsistencies in the TIA Act, as discussed below.

Correction of inconsistencies in the TIA Act

2.40 Several of the items in this Bill will, if passed, overcome drafting errors which have prevented subsections 16(1A) and 60(4A) of the TIA Act from operating.

2.41 Both sections of the TIA Act relate to the requirement to provide carriers with descriptions of devices added to a warrant. The sections are internally inconsistent in that they require the warrants to be in relation to a single identified device, but also indicate that additional devices, not identified in the warrant, can be added to the warrant.

2.42 For example, in relation to section 16, the internal inconsistency arises in that section 16(1A) provides that a certifying person must cause the Managing Director of the carrier to be given a description in writing of a device not identified in a warrant as soon as practicable. However, the warrant concerned is required to be a warrant that authorises the interception of a telecommunications device identified in the warrant. The requirement that the warrant has to be for an identified device means that the other conditions can never be satisfied, and the section is of no effect. It also has the effect that, under the TIA Act as it currently stands, it is not possible for a device-based named person warrant to include multiple telecommunications devices, or for devices to be added subsequent to the issuing of the warrant. However, there are some provisions in the Act that indicate this may have been the intention.

2.43 Item 14 (paragraph 2.37 above) will, if passed, substitute the words 'a telecommunications device, identified in the warrant' with the words 'any telecommunications device'. This would resolve the inconsistency. Item 37 will resolve the inconsistency in paragraph 60(4A)(b) of the TIA Act in a similar way.

Notifications of warrants to and by state ministers

Summary of provisions

2.44 Item 15 of Schedule 1 of the Bill will repeal paragraph 35(1)(b) of the TIA Act to remove a current mandatory requirement for a state interception agency to provide a copy of each warrant and instrument of revocation to the responsible state minister.[22]

2.45 Item 17 will amend paragraph 35(1)(e) of the TIA Act, removing the subsequent reporting requirements for the responsible state minister to provide a copy

22 EM, p. 5.

of the warrant or instrument of revocation to the commonwealth minister (ie: the Attorney-General).

2.46 The EM states that while the requirement for the state minister to provide copies of warrants and revocation instruments to the commonwealth minister was originally required as an accountability mechanism, this is now an unnecessary duplication. The EM explains the process for ensuring that the Attorney-General is notified of warrant issue and evocation[23]:

> Originally required as an accountability mechanism, the practice of the responsible State Minister providing copies of warrants to the Commonwealth Minister is now an unnecessary duplication. Following the passage of the Telecommunications (Interception) Amendment Act 2006 interception agencies are required to provide copies of warrants and revocations to the Secretary of the Commonwealth Attorney-General's Department, who in turn provides them to the Commonwealth Minister on a quarterly basis.[24]

The EM does not provide any further rationale for the removal of the mandatory requirement for the state minister to receive copies of all warrants and revocations.

2.47 Item 19 will insert a new subsection 36(1) that will allow state legislation to make provision for the relevant responsible state minister to receive a copy of each warrant and instrument of revocation, should the responsible state minister wish to do so. However, individual states must enact state law if the ministers concerned wish to exercise this option. Item 19 also provides that where a state enacts such legislation, disclosure of a copy of a lawfully issued telecommunications interception warrant to a responsible state minister is a lawful disclosure of such information.

Background

2.48 The items referred to in this section of the report have their origins in conclusions and recommendations made in the *Report of the Review of the Regulation of Access to Communications* by Mr Tony Blunn.[25]

2.49 In that report, Mr Blunn made a number of recommendations, including that the Agency Co-ordinator (Attorney-General's Department), rather than the AFP, be given responsibility for maintaining the register of warrants, their issue and revocation. This change was primarily implemented in the *Telecommunications (Interception) Amendment Act 2006.*

---

23 A copy of a revocation must be provided to the Secretary of the Department by either the Judge or nominated AAT member (paragraph 52 (2) (b)) or the chief officer of an agency (paragraph 57 (3) (b)) who revoked the warrant. Currently, the chief officer of an agency must cause a copy of the warrant to be given to the Secretary of the Department under section 53, although this section is to be repealed under item 27 and replaced at item 31 with new section 59A.

24 EM, p. 5.

25 A.S. Blunn AO, *Report of the Review of the Regulation of Access to Communications*, 2005.

2.50 In the process of arriving at this recommendation, Mr Blunn noted that the NSW Attorney-General had questioned the need for state ministers to be provided with copies of warrants, instruments and reports, as required by section 35 of the TIA Act. Mr Blunn noted that the implications of the NSW Attorney-General's comments were that the minister does not examine the warrants and instruments of revocation, but relies instead on compliance reports from the NSW Ombudsman.

2.51 While expressing apparent concern about whether the Minister was meeting the intention of the legislation by relying on such reports, Mr Blunn observed that 'it is difficult to see any useful purpose being served by requiring the State Minister to act merely as a conduit' and that 'it makes even less sense…that under the existing arrangements the Commonwealth….has already received and actioned copies'.[26]

2.52 Mr Blunn considered that the requirements imposed by section 35 would make sense if the intention of the state minister in forwarding the material to the Commonwealth was to endorse it and thereby accept responsibility for the actions of the state officers involved. He said, however, that whether or not this was the intention of the legislation is not apparent, and that the NSW Minister clearly did not think this was the case. Mr Blunn concluded that:

> In my view if that is the intention it should be made explicit and if not, and in the absence of some other explicit and agreed objective, the obligation on the State Minister should be removed.[27]

26 A.S. Blunn AO, *Report of the Review of the Regulation of Access to Communications*, 2005, p. 63.

27 A.S. Blunn AO, *Report of the Review of the Regulation of Access to Communications*, 2005, p. 68.