The Senate

Standing Committee on Legal and Constitutional Affairs

Telecommunications (Interception and Access) Amendment Bill 2008

May 2008

ISBN: 978-0-642-71907-2

This document was printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

MEMBERS OF THE COMMITTEE

Members
Senator Patricia Crossin, **Chair**, ALP, NT
Senator Guy Barnett, **Deputy Chair**, LP, TAS
Senator Andrew Bartlett, AD, QLD
Senator Mary Jo Fisher, LP, SA
Senator Annette Hurley, APL, SA
Senator Linda Kirk, ALP, SA
Senator Gavin Marshall, ALP, VIC
Senator Russell Trood, LP, QLD

Participating Members
Senator Bob Brown, AG, TAS
Senator John Hogg, ALP, QLD

Secretariat

Mr Peter Hallahan	Secretary
Ms Anne Withell	Principal Research Officer
Ms Hanako Jones	Executive Assistant

Suite S1. 61	Telephone: (02) 6277 3560
Parliament House	Fax: (02) 6277 5794
CANBERRA ACT 2600	Email: legcon.sen@aph.gov.au

TABLE OF CONTENTS

ABBREVIATIONS

AAT	Administrative Appeals Tribunal
AFP	Australian Federal Police
ASIO	Australian Security Intelligence Organisation
The Bill	Telecommunications (Interception and Access) Amendment Bill 2008
Blunn Review	*Review of the Regulation of Access to Communications* by Anthony Blunn AO, August 2005
Castan Centre	Castan Centre for Human Rights Law
Department	Attorney-General's Department
EFA	Electronic Frontiers Australia
EM	Explanatory Memorandum
IMEI	International Mobile Equipment Identifier (for a mobile telephone handset)
IMSI	International Mobile Service Identifier (for services)
Law Council	Law Council of Australia
MAC	Media Access Control (for a computer or any wireless connected device)
Privacy Foundation	Australian Privacy Foundation
TIA Act	*Telecommunications (Interception and Access) Act 1979*

RECOMMENDATIONS

Recommendation 1

3.18 The committee recommends 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.

Recommendation 2

4.86 The committee recommends that the recommendation at paragraph 3.2.5 of the Blunn report, which reads:

> **3.2.5. Accordingly, I recommend that priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.**

be adopted, and priority given to developing a unique and indelible identifier of the source of telecommunications.

Recommendation 3

4.87 The committee recommends that the Bill be amended to provide that an agency be permitted to add a device to a device-based named person warrant after the warrant has been issued if the facts of the case would have justified the issue of a warrant by the issuing authority; and the investigation in relation to the person named in the warrant will be, or is likely to be, seriously prejudiced if the interception does not proceed.

Recommendation 4

4.88 The committee further recommends that the Bill be amended to provide that if an agency adds a telecommunications device or devices not identified on a device-based named person warrant at the time that the issuing authority issued the warrant:

(i) the agency be required to notify an issuing authority, within 2 working days, that a device had been added to the warrant; and

(ii) the issuing authority must examine the supporting documentation against the criteria that it would have considered, in accordance with the requirements of the *Telecommunications (Interception and Access) Act 1979*, in relation to an application by the agency for a device-based named person warrant, and make a determination about whether the facts of the case justified the addition of the device; and

(iii) the issuing authority shall order that the interception cease immediately and that all evidence gathered be destroyed if it determines that the facts of the case would not have supported the issue of a device-based named person warrant.

Recommendation 5

4.89 The committee recommends that the Bill be amended to insert a requirement that the Annual Report in relation to the *Telecommunications (Interception and Access) Act 1979* incorporate the following additional information over and above that already required by the Act:

- **the number of service-based and device-based interceptions, to be reported upon separately but in a similar format to that currently used for the total number of intercepted telecommunication services; and**
- **the number of devices in the original warrant and the number of additional devices added to the warrant, reported in a similar format to that currently used for reporting the total number of intercepted telecommunications services.**

Recommendation 6

6.13 The Committee recommends that the Australian Government commission an independent review of the operation of the *Telecommunications (Interception and Access) Act 1979* within 3 years.

Recommendation 7

6.14 The Committee further recommends that the Australian Government introduce amendments to the *Telecommunications (Interception and Access) Act 1979* in subsequent legislation, to provide for a statutory requirement that the TIA Act be independently reviewed every five years.

Recommendation 8

6.15 Subject to the preceding recommendations the committee recommends that the Senate pass the Bill.

CHAPTER 1

INTRODUCTION

Referral

1.1 On 19 March 2008, following a recommendation of the Selection of Bills Committee, the Senate referred the Telecommunications (Interception and Access) Amendment Bill 2008 (the Bill) to the Standing Committee on Legal and Constitutional Affairs (the committee) for inquiry and report by 1 May 2008.

1.2 On 1 May 2008, the committee presented an interim report stating that the committee intended to present its final report on 6 May 2008.

Purpose of the Bill

1.3 The main purpose of the Bill is to amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act)[1] to extend sunset provisions that provide exemptions from the prohibition against listening to or copying communications passing over a telecommunications system. These exemptions allow specific law enforcement and security agencies to monitor all communications within their corporate networks, outside of a warrant regime, for the purpose of protecting and maintaining their networks and maintaining their professional standards.

1.4 The sunset provisions are due to expire on 13 June 2008. According to the Attorney-General's Second Reading Speech, the proposed eighteen month extension will enable law enforcement and security agencies to continue to protect their networks while a full legislative solution is developed.[2]

1.5 The Explanatory Memorandum (EM) states that the Bill also proposes additional amendments to improve the effectiveness of the telecommunications regime by:

- clarifying agencies' reporting requirements under the TIA Act;
- clarifying that multiple telecommunication devices can be intercepted on the one named person warrant; and
- making minor and technical amendments that arise from the transfer of duties from the Australian Federal Police (AFP) to the Attorney-

1 The TIA Act was renamed in 2006 from the *Telecommunications (Interception) Act 1979*.

2 The Hon. Robert McClelland MP, Attorney-General, House of Representatives Official Hansard, 20 February 2008.

General's Department (the Department) consequent to the passage of the *Telecommunications (Interception) Amendment Act 2006*.[3]

Conduct of the inquiry

1.6 The committee wrote to 65 individuals and organisations inviting submissions by 9 April 2008. Details of the inquiry, the bill and associated documents were also placed on the Committee's website.

1.7 The committee received 14 submissions. These are listed at Appendix 1. Submissions were placed on the committee's website.

1.8 The committee held a public hearing in Sydney on 17 April 2008. A list of witnesses who appeared at the hearing is at Appendix 2 and copies of the Hansard transcript are available on the committee's website.

Acknowledgement

1.9 The committee thanks those organisations and individuals who made submissions and gave evidence at the public hearing.

Note on references

1.10 References in this report are to individual submissions as received by the committee, not to a bound volume. References to Committee Hansard are to the proof Hansard: page numbers may vary between the proof and the official Hansard.

3 EM, Telecommunications (Interception and Access) Amendment Bill 2008, p. 1, http://parlinfoweb.parl.net/parlinfo//view_document.aspx?TABLE=EMS&ID=2897

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.

CHAPTER 3

EXTENSION OF NETWORK PROTECTION SUNSET DATES

3.1 Several submissions commented on the proposed extension of the sunset clauses for network protection exemptions. When these provisions were first introduced to Parliament in the Telecommunications (Interception) Amendment Bill 2006, the Minister stated that network protection was an issue for both public and private organisations and that a policy proposal to allow appropriate, lawful access for network administrators was the subject of ongoing consultation. Since then these provisions have been amended only to allow additional law enforcement agencies, not corporate agencies, to be exempt under the provisions.

3.2 The Law Council of Australia (Law Council) submission noted that sunset clauses are included in legislation for a number of purposes, including to:

- ensure that certain legislative provisions only remain in operation as long as is necessary to address a temporary emergency situation;
- compel the periodic review of the operation of a controversial provision; and
- provide a temporary measure to respond to a particular problem, while a more permanent solution is developed.[1]

The Law Council noted that the sunset clauses relating to network protection fulfil the third purpose.

3.3 In submissions to the inquiry, the Australian Privacy Foundation and the Law Council proposed that consideration of a further extension of the sunset clauses relating to network protection should be based on further information. In particular, these parties contended that the Senate should be provided with information on progress toward a more permanent solution, particularly for corporate entities, on why such a solution is not in place, and whether and why a further eighteen months is required.

3.4 Addressing the issue of progress towards a longer-term solution, the Attorney-General's Department submitted that:

> While significant progress has been made by the Department towards a full legislative solution, the additional 18 months will allow adequate time to finalise the policy development and undertake consultation with state and territory governments and a broad range of non-government stakeholders.

---

1 *Submission* 1, p. 14.

> The additional 18 months will also allow for any issues raised during these consultations to be fully considered and incorporated where appropriate.[2]

3.5 When asked by the committee about the extent of progress to develop a long term solution, the Attorney-General's Department responded:

> We have been developing a discussion paper which has not gone outside the Attorney-General's Department. What has become clear, as we look into the problem, is that technology is moving very quickly. The types of threats to critical infrastructure are changing every single day and so we are looking at the scope of any possible solution to address the kinds of challenges that we are dealing with. We work with our critical infrastructure protection area in the department very closely and it is with them that we are actually looking at the scope of any solution.[3]

3.6 In relation to why the Department needed a further 18 months for the process, representatives said that:

> …essentially we are taking into that time the fact that we have just had an election so that slowed down any development of a particular policy. Now we want to ensure that we develop a solution that allows us to consult very broadly because there are a lot of stakeholders who will be affected by any change in legislation. We want to ensure that we do not need a further extension of time, so that is why we have sought 18 months.[4]

3.7 The committee also sought information from government representatives on whether corporate agencies may be in technical breach of the TIA Act in their current practices for virus scanning and email quarantine systems. A representative of the Attorney-General's Department acknowledged that this is a grey area, stating:

> The nature of computer networks is so different and complex that I could not comment on whether particular areas of industry or banking or whatever would be in technical breach of the act. What I can say is that when it is appropriate we constantly provide guidance to organisations when they ring up and talk about their filtering systems. You will find that a lot of organisations actually straightaway block emails of a particular attachment type because they know that they are likely to have problems embedded, even though they might be quite innocent. They also run electronic scanning, which is not in breach of the legislation. But we have identified that this is an area that is grey and that needs to be dealt with as quickly as we can. Certainly I am not aware of any organisation that is in technical breach of the legislation. As I have said, we welcome people to approach the department and seek guidance on how they can actually act and not be in breach of the legislation and still protect their networks.[5]

---

2 *Submission* 4, p. 2.

3 *Committee Hansard*, 17 April 2008, p. 28.

4 *Committee Hansard*, 17 April 2008, p. 28.

5 *Committee Hansard*, 17 April 2008, p. 35.

3.8 The committee also sought to clarify with other witnesses whether they had any specific concerns with the amendments relating to extension of the sunset dates contained in the Bill. A number[6] supported the submission of the Office of the Privacy Commissioner (OPC), which stated that:

> The Office supports the position of the Blunn Review that network protection provisions should be accompanied by appropriate privacy protections. Further, in the view of the Office, the subsequent widening of the scope of the network protection exemption to over 20 agencies makes it more important that the safeguards recommended by the Blunn Review are built-into the legislation, including for the purposes of the proposed 18 month extension to the sunset provisions.[7]

3.9 In relation to privacy protections, the OPC recommended that consideration be given to amending the Bill to contain the following more rigorous requirements:

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

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

(c) that any data obtained for the purpose of network security should be immediately destroyed when it is no longer needed for that purpose.[8]

3.10 The committee notes that recommendation (b) is consistent with findings in the Blunn report. Both the OPC and the Blunn report also proposed a higher level of personal privacy protection for network protection provisions than is currently enshrined in the TIA Act. However, while their issues and recommendations are not mutually exclusive, the Blunn report raises additional issues in regards to voice data and evidence discovered in relation to criminal behaviour:

> 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 [Carriage and Carriage Service Providers] are required to protect data accessed in the course of their employment. The vexed question is what should happen where such access discloses evidence of criminal behaviour. … In my view in both situations the content of the communication should be protected but the person with access may report their view that there may be evidence of criminality etc. The data, presumably other than voice data, could then be accessed as if it were a stored communication i.e. by search warrant. The question of the use of the content of voice data raises

6 Submissions 1, 8, 10.

7 Office of the Privacy Commissioner, *Submission* 7, p. 5.

8 Office of the Privacy Commissioner, *Submission* 7, pp 4-6.

significant evidentiary and other problems and should be separately considered.[9]

Committee findings and recommendations

3.11 The committee is aware of the rapidly changing nature of technology and of the sensitive nature of data held by security and law enforcement agencies. These agencies consequently face challenges in maintaining secure networks and professional standards—both of which the community expect them to maintain in a manner that safeguards rights, privacy and safety.

3.12 While developing 'technologically neutral' legislation may be difficult, almost eighteen months have passed since the sunset clauses were approved by Parliament. This timeframe was apparently established to allow the Attorney-General's Department to develop a full legislative solution to network protection issues for corporate entities and interception agencies.

3.13 Additionally, the Blunn report had proposed in 2005 that the network protection provisions should address both corporate and interception agency needs, and had raised a number of issues that needed to be resolved in terms of privacy and secondary data use. The issues raised by the Blunn report were not addressed in the Telecommunications (Interception) Amendment Bill 2006, partly due to its late insertion into the parliamentary program, and were also not addressed when additional agencies were given network protection exemptions in 2007.[10]

3.14 The committee considers that the recommendations made in the submission to this inquiry by the Office of the Privacy Commissioner in relation to privacy issues warrant further consideration, along with the unresolved issues raised in the Blunn report.

3.15 Since the Blunn report, the committee has now been asked on three occasions to consider the network protection issue, with little or no information being provided on the impacts on privacy and agency accountability. Furthermore, the so-called 'grey area' of monitoring and interception of data in corporate networks does not appear to have progressed beyond a draft policy within the Attorney-General's Department.

3.16 The committee considers that any future legislative amendment of the network protection provisions (including sunset clauses) 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.

---

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

10 These measures were contained in the *Telecommunications (Interception and Access) Amendment Act 2007.*

3.17 However, the committee considers that these issues can not be adequately addressed by amending the Bill, given the imminent expiry of the sunset clauses. Further, implementing a single change to ensure that the person to which the exemption applies is clearly identified would be an incomplete solution, which might reduce the likelihood of this issue being resolved in a more comprehensive way.

Recommendation 1

3.18 The committee recommends 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.

CHAPTER 4

DEVICE-BASED NAMED PERSON WARRANTS

4.1 A broad range of witnesses raised concerns in relation to the proposal in the Bill to permit devices to be added to a warrant after it had been issued and without further reference to the issuing authority, and for the identification of devices in warrants only to the extent that it is known. These witnesses, which included the Law Council of Australia (the Law Council), the Castan Centre for Human Rights Law (Castan Centre), Privacy Commissioners and civil liberties groups, (collectively privacy and civil liberties groups), considered that the proposed amendments represented an extension of interception powers that would result in innocent persons who were not the subject of investigation having their privacy invaded. These concerns are discussed in greater detail below, under the following broad subject headings:

- Tension between privacy rights and the need for interception powers;
- Identification of devices;
- Adding devices to device-based warrants after issue;
- Accountability mechanisms;
- Consistency between service-based and device-based warrants;
- Legislative intent concerning device-based named person warrants; and
- Suggestions for safeguards if devices are added to warrants.

4.2 The chapter incorporates committee conclusions in each section where appropriate.

The tension between privacy and the need for interception powers

4.3 Evidence heard by the committee was primarily divided between two viewpoints. Submissions by police forces[1] and the Attorney General's Department (the Department) considered the amendments were needed by interception authorities for operational purposes. Conversely, privacy and civil liberties groups considered the amendments unsatisfactory in relation to the protection of individuals' rights to privacy and public accountability standards.

4.4 The committee received evidence that the impact from a privacy perspective was significant and potentially inconsistent with community expectations. For example, the Victorian Privacy Commissioner submitted that:

> The effect of this bill on the privacy of individuals is significant.

---

1 *Submission* 9, pp 1-3; *Submission* 12, pp 1-3; *Submission* 13, pp 1-2; *Submission* 14, p. 1.

> With the increase in uptake and use of technology, communication over the internet and telephones (including mobile phones) is the primary method of communication today. Individuals communicating through telecommunications devices are likely to exchange all sorts of information, ranging from private health information to personal business affairs, the nature of professional advice received as well as sensitive information concerning their health, sexual orientation and practices, political opinions and religious views.
>
> Australians have the right to expect that the State will not intercept or access their communications without just cause and due process. The greater impact a warrant will have on an individual's rights (including their right to privacy), the more stringent the requirements for obtaining the warrant should be. If granted, any warrant should be as specific, finite and limited as is reasonable in achieving its aims. In particular, the ability of the warrant system to protect individual privacy depends on the issuing authority considering each individual device from which telecommunication are to be intercepted under the warrant.[2]

4.5 Conversely, while acknowledging privacy issues, the Victoria Police's submission expressed its need for these amendments from a law enforcement viewpoint:

> There is clearly an operational need for Law Enforcement Agencies to be able to obtain a single warrant which authorises the interception of multiple devices used or likely to be used by the suspect and which allows additional devices to be added to a warrant if and when they are identified. …
>
> Service-based named person warrants exist to allow multiple services to be intercepted in connection with one named person warrant and also additional services to be added to a warrant if and when they are identified. The proposed amendment will allow the provisions governing the issue of device-based named person warrants to be brought into line with the provisions governing the issue of service-based warrants.
>
> The expanding use of telecommunication interception powers as an investigative tool and the associated concerns that this may give rise to, such as issues of privacy and the expansion of police powers, are always relevant factors. However, the amendment merely provides a means of obtaining evidence in a more timely manner than is currently possible under existing legislation.[3]

4.6 Representatives of the Department explained that interception agencies need the operational flexibility to adapt to changing technology, noting that while the legislation is intentionally technologically neutral, changes in technology have required legislative amendment to maintain operational effectiveness:

---

2 *Submission* 5, p. 2.

3 *Submission* 9, p. 2.

> Advances in technology have created a market where multiple communications are the norm due to the low cost associated with purchasing telecommunications services. This is creating an environment whereby it is reasonably inexpensive to purchase multiple communications devices such as mobile phone handsets or laptop computers. These devices, when combined with the availability of multiple services, provide opportunities for evading detection by law enforcement agencies…
>
> …
>
> To meet community expectations that serious criminal offences are investigated and prosecuted, it is important that law enforcement [and] national security agencies can quickly adjust to this changing environment.[4]

4.7 The committee acknowledges the tension between the need for interception agencies to have the necessary powers to safeguard the community; and the requirement to protect individuals' rights to privacy, particularly those persons who are not associated with a particular investigation. These objectives need to be balanced in any legislative amendment that involves new powers, or an extension of powers.

Identification of devices

4.8 The accurate identification of telecommunications devices to be intercepted is contentious because of the potential to intrude upon the privacy of innocent people if devices are not correctly identified before interception commences. The submission made by the Law Council illustrated two examples of how an unjustified invasion of a person's privacy might inadvertently occur:

> ASIO or a law enforcement agency may have correctly identified their suspect *but* may have erroneously identified the telecommunications services or devices used by that person, (again perhaps on the basis of incomplete or unreliable information), with the result that the communications of an innocent third party are intercepted.
>
> ASIO or a law enforcement agency may have correctly identified their suspect and correctly identified the telecommunication service or devices used by that person *but* may not be technically able to uniquely identify telecommunications made using that service or device without the risk of intercepting communications made via an unrelated service or device (This appears to be more of a real risk with device-based, rather than service-based interception…).[5]

4.9 The Law Council concluded that 'the proposed amendments will significantly reduce the role of the warrant authorisation process in safeguarding against errors of the kind…' illustrated above.[6]

---

4 *Committee Hansard*, 17 April 2008, p. 28.

5 *Submission* 1, p. 4.

6 *Submission* 1, p. 8.

4.10 In relation to identification of devices, several submissions[7] drew the committee's attention to previous examination of this issue in the Blunn report;[8] the committee's previous findings and recommendations in relation to the introduction of device-based warrants in the 2006 amendment bill; and/or the subsequent government response. These submissions questioned whether there had been further development to improve the reliability and accuracy of unique identifiers that the Australian Government had committed to progress, or whether this commitment was now being put aside.

4.11 For example, the Law Council submitted that:

> There is no information included in the material supporting the Bill to suggest that the concerns expressed by the Senate committee in 2006 about the accuracy and reliability of device based interception have been addressed. Nonetheless, the proposed amendments explicitly invite Parliament to treat device-based interception as no more risky or problematic than service based interception.[9]

4.12 The Department stated that unique identifiers are available for devices such as mobile handsets and laptops:

> All telecommunications devices, such as a mobile handset or a laptop computer, have a unique identifier that allows the device to interact with telecommunications. For example, the unique identifier for a mobile handset is called an International Mobile Equipment Identifier (IMEI). A unique identifier for a computer or any wireless connected device is a Media Access Control (MAC) address. It is possible to match the unique identifier of the device to a particular person via subscriber detail or through the monitoring of known telecommunications services that the person of interest is using.[10]

4.13 However, the committee also received evidence from the Department which suggested that accurately identifying a unique and indelible identifier of the source of telecommunications, as recommended in the Blunn report, remains an operational challenge. The Department provided the following scenario:

> There will be intelligence to say someone has walked into a particular shop and bought half a dozen phones plus 100 SIM cards, which is not an unusual scenario. The reality is, that until they use the phone, you cannot identify the unique identifier.[11]

---

7 Submission 1, p. 4; *Submission* 7, pp. 6-7; *Submission* 10, p. 2.

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

9 *Submission* 1, pp 5 and 7.

10 *Submission* 4, p. 3.

11 *Committee Hansard*, 17 April 2008, p. 33.

4.14 Further, there appears to be some doubt about the reliability of the unique device identifiers, due to the possibility that these may be altered. At the public hearing, a representative of Electronic Frontiers Australia (EFA) advised that altering the identification of a device was possible:

> In many if not most cases, those [device-based] identifiers can be altered, cloned or copied, so that they do not reliably provide a unique identifier. Moreover, we are given to understand that where suspects in criminal investigations, for example, might be seeking to avoid surveillance by law enforcement agencies, they might be minded to change identifiers to hide their tracks. In the types of situations in which these warrants might address this, there is perhaps a higher than normal chance that identifiers might not be unique.[12]

4.15 The Department acknowledged this concern, stating that:

> In a policy sense, we are working with the industry, ACMA [Australian Communications and Media Authority] and the Department of BCDE [Broadband, Communications and the Digital Economy] to look at ways to deal with this problem. There are offences in the Criminal Code for altering IMEIs [International Mobile Equipment Identifiers] and IMSIs [International Mobile Service Identifiers]—being the service number or the actual phone handset number—and the AFP [Australian Federal Police] enforces those particular laws in relation to changing IMEIs and IMSIs. But, of course, technology is very fast moving and people will always find ways to change numbers.[13]

4.16 The New South Wales Council for Civil Liberties (NSWCCC) submitted that allowing more devices to be intercepted without improving device identification accuracy was not acceptable on privacy grounds:

> A significant number of additional people will have their conversations and other messages listened to or read if this Bill is passed. These will include users of intercepted devices other than the targeted person, and those with whom they communicate. Until such time as devices are identifiable by unique identifiers and accidental interception of the wrong devices is eliminated, they will also include persons not connected in any way with the targeted person. The broader the range of devices which are targeted, the greater the increase in invasion of privacy.[14]

Adding devices to device-based warrants after issue

4.17 A major change proposed in the Bill relates to allowing interception agencies to add additional devices to a device-based warrant without further referral to an issuing authority. Many of the submissions and much of the evidence received at the

---

12 *Committee Hansard*, 17 April 2008, p. 18.

13 *Committee Hansard*, 17 April 2008, p. 34.

14 *Submission* 2, pp 2-3.

hearing objected to this proposed change, viewing it as a major extension of the existing provisions.

4.18 The following section of this report is laid out as follows:

- Paragraphs 4.19 – 4.22 set out a description, as primarily incorporated in the Attorney-General's Department's submission, of how privacy issues will be addressed and how accountability mechanisms will operate;
- Paragraphs 4.23 – 4.26 describe operational practices and needs, as put forward in evidence by police forces.
- Paragraphs 4.27 – 4.30 then return to the objections raised by privacy and civil liberties groups.

Requirements, process and safeguards

4.19 The Department described the existing two-tier process to address privacy in the issuing process for a device-based named person warrant. The first step is to establish that a device-based named person warrant is the only practical mechanism available to intercept telecommunications:

> The primary issue of the interference with a person's privacy is addressed by the issuing authority in considering whether to grant a device-based named person warrant. The interception agency must satisfy the issuing authority that:
>
> - there are no other practicable methods available at that time to identify the telecommunications services being used, or likely to be used, by the person of interest, or
> - it is impracticable to intercept the service being used by the person of interest.[15]

4.20 If the issuing authority is satisfied that a device-based named person warrant is appropriate to the circumstances, the issuing authority then must have regard to the following privacy considerations and other factors:

> - the impact the interception will have on the existing privacy of any persons as a result of intercepting communications made from any service or of a particular device used or likely to be used by the person of interest;
> - the extent to which alternative methods of investigation have been used by the interception agency; and
> - that the interception is for an investigation of a serious offence, generally punishable by a maximum period of imprisonment of at least seven years.[16]

---

15 *Submission* 4, p. 3.

16 *Submission* 4, p. 3.

4.21 The Department's submission also explained the internal procedures to which an interception agency would be required to adhere if the agency was permitted to add additional devices to a warrant without independent external scrutiny:

> The Bill allows the head of an agency or a senior officer or staff member of an agency who has been approved in writing by the chief officer of an agency, to approve the addition to the warrant of an additional device, and to notify the relevant carrier. The senior officer is not able to make decisions that go beyond the limits of the original warrant and therefore is required to be satisfied that the addition of a device to a named person warrant would meet the thresholds that an issuing authority must have regard to, or be satisfied of, in issuing the original warrant.[17]

4.22 The submission went on to explain the existing accountability mechanisms under the TIA Act that would be safeguards which might address issues raised by privacy and civil liberties groups:

- An interception agency is required to revoke a warrant when the grounds for the warrant no longer exist. This includes where it is no longer impracticable to intercept telecommunications being used by the person.
- Intercepted material must be destroyed where it is not relevant to the permitted purposes of the agency – generally an investigation of an offence that is punishable by three years imprisonment or more.
- An issuing authority may impose conditions or restrictions on an interception warrant.
- The Ombudsman has independent oversight of the conduct of the interception agencies in carrying out interception.[18]

Operational need for devices to be added after issue of the warrant

4.23 The committee received evidence from Victoria Police, the AFP and the Attorney-General's Department that operational effectiveness requires the timely interception of devices since:

> The evolving practice by the criminal element of utilising multiple SIM cards in multiple handsets has become a significant inhibitor to the detection of crime and the apprehension of offenders. LEA's [law enforcement agencies] once again will be at a disadvantage when trying to identify and subsequently intercept telecommunications in a timely manner. The 'educated' criminal element is already utilising such practices to defeat current methods of telecommunications interception and will continue to do so. The use of such tactics will certainly increase as it becomes more commonly known.[19]

---

17 *Submission* 4, p. 4.

18 *Submission* 4, p. 4.

19 *Submission* 9, p. 2.

4.24 Tasmania Police also noted that the amendments would 'provide for a greater effectiveness of the Telecommunications Interception warrant regime'.[20]

4.25 A representative of the AFP described the warrant process and need for timeliness to the committee from an operational perspective:

> …when you are seeking the grounds for the original warrant, you are at the earlier stage of the investigation. You do not have interception in place, so you are going through that accountability process. I do not think that anything we are saying or the department is saying is meant to undermine the importance of that up-front authorisation by an external body. What we are talking about is the fact that, in the overall architecture of the T(I) Act [TIA Act], a device based warrant is in the first place really the warrant of last resort. We have to be satisfied, and we need to be able to satisfy our internal processes and then the issuing authority, that a service based warrant or some other TI [telecommunications interception] warrant is not a better way to get access to the information that we are after to assist with our investigation. As that investigation progresses and we are aware or become aware that that person suspects that they are under surveillance by the police, that the police are interested in them, and they start undertaking those counter surveillance type activities, we need to be able to try and counter that to maintain our capability. That is why we are suggesting that, when it comes to adding a device to an existing warrant where we were not aware of the existence of that device when we first sought the warrant, an internal authorisation approach, on balance with the other accountabilities that are available in the Act, is the best way ahead from an operational perspective.[21]

4.26 A representative of the Department also described some of the internal accountability and approval requirements that will apply when a device is to be added subsequent to the issue of a warrant:

> …the decision to add another device will be made by a senior officer within the agency, which does sit separately from any of the actual investigation itself, so the objectivity does come in there. I should also say that they will not be able to add a device that is inconsistent with the purposes of the warrant in the first instance. There has to be not only the likelihood that the person is using it but the likelihood that the use of it is in relation to the offence for which the warrant was issued.…
>
> I should also say that, as a matter of best practice, the Attorney-General's Department must receive copies of all warrants.[22]

---

20 *Submission* 13, p. 2.

21 *Committee Hansard*, 17 April 2008, p. 33.

22 *Committee Hansard,* 17 April 2008, p. 31.

Scrutiny of devices added to a warrant

4.27 The committee heard evidence arguing that the provisions of the Bill that will permit interception agencies to add new devices to a warrant without further independent scrutiny by the issuing authority would adversely affect the privacy rights of individuals.

4.28 The Law Council firstly agreed with the statement in the Department's submission that 'the primary issue of the interference with a person's privacy is addressed by the issuing authority in considering whether to grant a named person warrant.'[23] However, the Law Council went on to state that:

> …it is difficult to see how the threshold test for privacy can be met where the issuing authority remains unaware of the particular devices to be targeted under the warrant.[24]

4.29 The Castan Centre elaborated on the privacy consequences of removing the requirement that an issuing authority scrutinise information pertaining to all devices in a warrant:

> At the time of issuing, the issuing authority does not know what those devices are or might be and so has no basis on which to adequately address the question of whether or not the interception of those further devices would interfere with the privacy of any person or persons in an inappropriate fashion. The concern arises particularly in relation to device based warrants because when one looks, for example, at the explanatory memorandum for the 2006 bill, which introduced the device based warrants, it makes it clear that the logic of a device based warrant is that it is useful when a device is being used in respect of multiple services. Of course the device might also be used by multiple users.
>
> So… it seems quite possible that some person, not of interest to the authorities and who was not identified in the warrant, might nevertheless be using the device to make a communication on some service or other and then become subject to interception pursuant to the warrant.[25]

4.30 The committee questioned several witnesses about whether the requirement to seek prior approval from an issuing authority before adding devices to a warrant imposed an additional 'red tape' burden on an interception agency, in terms of time and identifying the device. Witnesses were consistent in considering that prior approval is appropriate and necessary. Comments included:

- the 'red tape' includes existing safeguards and there is a significant difference between extra red tape and the removal of safeguards;[26]

---

23 *Submission* 1, p. 10.

24 *Submission* 1, p. 10.

25 *Committee Hansard*, 17 April 2008, p. 3.

26 *Committee Hansard*, 17 April 2008, p. 24.

- the requirement to seek approval is consistent with Australia's international human rights obligations;[27]
- there is a balance to be struck between the lawful interception needs of an agency and the needs of the public to be protected from the excesses and abuses to which those powers could conceivably be put. The purpose of device-based warrants is to address the issue of 'proliferation of SIM cards', that is, the ability to intercept multiple SIM cards in one device;[28]
- the proposed amendment is fundamentally inconsistent with the nature of the independent review. An analogy for this proposal is that of a magistrate issuing a search warrant that allowed the police not only to search a residence of a particular suspect but any other place in which it is 'likely' a person might be. It removes the need for showing proof and justification before an independent party;[29]
- the one additional step of obtaining a warrant should not be omitted, as the AFP states in its submission that interception agencies are required in any case to do the work to identify the additional devices;[30]
- none of the current safeguards prevent interception agencies doing their jobs;[31] and
- the community would expect that a documented case needs to be made to someone to justify the addition of a device, and that case should preferably be made to someone external, rather than internal to the agency actioning the warrant.[32]

Conclusions

4.31 The committee acknowledges that interception effectiveness needs to keep pace with technological changes and changes in the behaviour of criminals seeking to avoid detection. This may require ongoing legislative change unless more 'technologically neutral' legislation can be introduced.

4.32 The committee accepts that even a short delay may result in loss of valuable information and affect investigatory outcomes. This is clearly not ideal and, in certain circumstances such as life-threatening situations, may be unacceptable. However, any changes to existing powers and safeguards must always be weighed against the potential for additional intrusion into individual rights and privacy.

---

27 *Committee Hansard*, 17 April 2008, p. 8.

28 *Committee Hansard*, 17 April 2008, p. 20.

29 *Committee Hansard*, 17 April 2008, p. 20.

30 *Committee Hansard*, 17 April 2008, p. 8.

31 *Committee Hansard*, 17 April 2008, p. 24.

32 *Committee Hansard*, 17 April 2008, p. 12.

4.33 The committee accepts that the ability of interception agencies to rapidly respond to 'turnover' in the telecommunication devices being used by people being intercepted is somewhat constrained by the current device-based warrant regime. This problem would be reduced if interception agencies were able to apply for multiple devices in a single application for a warrant. Allowing agencies to add devices to a warrant subsequent to its issue may also increase the capacity of interception agencies to respond in an efficient and timely manner. However, the TIA Act does not currently permit either process.

4.34 The committee is of the view that as a general principle, it is unobjectionable for interception agencies to intercept multiple devices on a device-based named person warrant. The committee is not convinced, however that an issuing authority can adequately consider potential interference with the privacy of any person(s), and also consider the other factors against which this should be balanced, if it is unaware of the identity of the devices that an interception agency may add subsequently to a device-based named person warrant.

4.35 During the course of the inquiry, Departmental representatives argued that replacing external scrutiny of devices that an interception agency wishes to add to a device-based named person warrant with internal-to-department scrutiny would still achieve equivalent consideration of privacy issues. The Department explained that the officer who will assess applications for additional devices would not be from within the area where the application originates. Additionally, the Department asserted that the purpose of the interception of the additional device must be consistent with that in the original warrant, and that each device is subject to the same test of 'likelihood' that the person named in the warrant is using the device.

4.36 However the committee considers that these safeguards cannot fully substitute for independent scrutiny by an issuing authority. The amendments, if passed, would remove an important existing safeguard, that is, independent scrutiny of any devices that an interception agency wishes to intercept.

4.37 Privacy Commissioners, civil liberties and rights groups and the Law Council were unanimous in considering that independent scrutiny is not merely 'red tape'. In their view, removing an existing safeguard is different from objecting to new safeguards. The committee agrees with this view and, in particular, considers that:

- compared with service-based interception, device-based interception is more likely to result in the invasion of privacy of people not identified in the warrant;
- a balance should be maintained between the protection of the community by security and law enforcement agencies; and the accidental or deliberate infringements on privacy that can result from interception; and
- independent review should be an integral part of the balancing effect of these interception powers on other public rights.

4.38 However, the committee considers that intercepting agencies should only be permitted to add further devices to a device-based named person warrant after the warrant has been issued in defined circumstances, not as a general practice. Any devices added should be notified to the issuing authority within a limited period. The issuing authority should also have the power to declare that the interception should cease and all information gathered destroyed if the issuing authority decides that the facts of the case would not have justified the addition of the devices.

Accountability mechanisms

4.39 The Law Council disagreed with the Department's statement that existing accountability mechanisms are sufficient safeguards for these proposed amendments. The Law Council did not find these mechanisms satisfactory, commenting specifically that:

> All but one of these accountability mechanisms are directed at monitoring the use of interception powers after a warrant has been issued and executed.
>
> The Law Council submits that 'after the fact' reporting or oversight mechanisms are not an adequate substitute for a rigorous, external warrant regime which determines whether, when and how ASIO or police should be exercising interception powers in the first place.[33]

4.40 A representative of the Privacy Foundation, after being questioned by the committee on whether the privacy protections outlined by the Department were sufficient, said:

> There are two types of privacy safeguards: those inherent in the authorisation process and the downstream safeguards. It is true that the downstream safeguards in terms of reporting and the necessity to comply with certain record-keeping requirements will still apply, but the upstream safeguards, the ones that are delivered by the authorisation process, are in a sense negated by a multiple device based warrant because the issuing authority is simply not in a position to make the appropriate judgement about the balance of interests since they will not have any information, as we understand it, about which other individuals may be users of those devices. Therefore, the arguments about the likelihood of the suspect or the target using those is information that simply will not be made available to an issuing authority so that they can make the appropriate judgement about the balance of interests.[34]

4.41 The Castan Centre discussed the effect of removing independent scrutiny and broadening the range of telecommunications devices from which communications may be intercepted. They said that the effect would be to dilute the statutory obligations of interception agencies to justify interceptions. The Castan Centre commented that:

---

33 *Submission* 1, p. 11.

34 *Committee Hansard*, 17 April 2008, p. 23.

> One potential consequence of such a dilution of accountability would be to encourage the undertaking of 'fishing expeditions', as agencies become freer to form their own, untested, views as to which devices a person is likely to use. This also further exposes the communications of third parties, not named in the warrant, to the possibility of interception, which is objectionable…[35]

4.42 A representative of the AFP disagreed with this view, commenting that internal safeguards and accountability mechanisms are sufficient:

> We believe that, for the addition of a device to an existing warrant, the internal accountability would be the way to go, and those additional oversight mechanisms would be through the reporting arrangements and the oversight of the Ombudsman and its scrutiny of our processes, which is fairly regular. It is annual and regular.[36]

4.43 The Castan Centre's submission identified several areas where dilution of accountability has resulted in cases which 'strongly suggest that investigatory agencies need to be held more accountable in the exercise of their statutory powers, not less so.'[37] The submission emphasised that this was not just about protecting human rights, but also about preserving agencies' integrity, and requiring them to account for the exercise of their powers.

4.44 The Castan Centre provided two examples to support its argument:

- the recent arrest and subsequent release of Dr Mohammed Haneef; and
- the case of Izhar Ul-Haque, in which the judgement of Justice Adams of the New South Wales Supreme Court criticised the conduct of both ASIO and AFP officers.

4.45 The representative of the Privacy Foundation provided other examples of internal scrutiny and accountability failure, citing the leakage of information and its misuse by officers of the Australian Taxation Office and Centrelink. He also drew attention to what he described as the 'fairly regular' instances of police corruption and misuse of official information, mainly in state police forces.[38]

4.46 The representative of the Privacy Foundation argued that these types of occurrences did not give the confidence 'to simply sweep away the safeguards in the name of efficiency.' He went on to differentiate between the abuse of information and the 'more general, chilling effect of surveillance' as follows:

> We think one of the dangerous trends is the tendency of governments to assure us that extension of powers to monitor and surveil the activities of

---

35 *Committee Hansard*, 17 April 2008, p. 5.

36 *Committee Hansard*, 17 April 2008, p. 33.

37 *Submission* 8, p. 6.

38 *Submission* 10, p. 24.

> citizens is okay because, as they say, they will put in place the safeguards that deal with the abuse and suchlike. That, to our view, negates the important social value of privacy and freedom from surveillance as something that we actually treasure and, in most liberal democracies, value quite highly. It simply is not good enough to say, 'If you've got nothing to hide you've got nothing to fear.' We all have the right, in our view, to basically go about our business in private unless it needs to be intruded on. The threshold tests for that intrusion need to be kept as high as possible.[39]

Conclusions

4.47 The committee is of the view that 'after the fact reporting' is insufficient to adequately address issues associated with individuals' privacy and rights.

4.48 In regards to the accountability mechanisms internal to interception agencies, the committee commends the work done by interception agencies to improve their processes and accountability mechanisms. However, the internal processes of any agency, public or private, are susceptible to failure, whether this be accidental, by oversight or omission, or deliberate. The care and attention to preserving a (possibly unknown) individual's right to privacy can be lost in the pressure of work and the need to achieve results.

4.49 The committee considers that best practice is to maintain independent scrutiny, should agencies be authorised to add devices to a warrant, except in exceptional circumstances.

Consistency between service- and device-based warrants

4.50 The EM for the Bill states that the changes to the device-based warrant provisions establish a consistency with the service-based warrant provisions.[40] The committee concurs that the proposed amendments will, if passed, establish a consistency or equivalency in terms of wording.

4.51 While the police forces and the Department did not specifically identify why this consistency is desirable, they drew attention to the operational needs of interception agencies (as outlined above) and, by inference, the need for the device-based and service-based provisions to be consistent. The Department and the AFP confirmed that the current requirement for an issuing authority to scrutinise every telecommunications device added to a device-based named person warrant would be removed by the Bill. However, they argued that the current safeguards and accountability mechanisms contained in the TIA Act, together with internal guidelines and procedures within agencies, would be sufficient to ensure privacy and accountability issues are adequately addressed.

---

39 *Submission* 10, p. 24.

40 EM, p. 4.

4.52 The committee heard evidence from privacy and civil liberties groups and the Law Council that device- and service-based interception warrants are not similar in nature and that relaxing provisions for devices to achieve 'consistency' with services is undesirable. In particular, these groups considered that device-based warrants were more likely to lead to the invasion of privacy and civil rights than service-based warrants. These groups concluded that independent scrutiny of devices added to a warrant is necessary, at the very least.

4.53 The committee acknowledges that accurate identification of devices remains more difficult than for services, and inaccurate identification may lead to the interception of the communications of people who not relevant to the investigation. Compared with services, devices are also more susceptible to having their identification tampered with or 'stolen', and devices are easier to dispose of and replace, as outlined above.

4.54 The Castan Centre submitted that another difference between services and devices is the multi-user nature of devices compared with services, which will potentially lead to more non-suspects being intercepted on a particular device than a particular service. The Castan Centre concluded that amending device-based warrant provisions to make them consistent with service-based interceptions would increase interception powers, as follows:

> One significant consequence of this broadening of the range of telecommunications devices from which communications may be intercepted would be to permit further incidental monitoring of people who are themselves of no relevance to a particular investigation, but who happen to use a telecommunications device that is 'likely' to be used by a person named in an interception warrant. This may be particularly so in relation to personal computers that are open for public use (eg in public libraries or internet cafes). By way of contrast, a service-based named person warrant may well not authorise interception of all communications from such a device, as many of the users of such a device may not be using it to communicate via a service that the person named in the warrant is using or likely to use. Therefore, these amendments would increase the power of interception, and not merely establish an equivalence between device and service-based warrants.[41]

Legislative intent concerning device-based named person warrants

4.55 The Department expressed the view that the Bill 'clarifies' the original intent of the 2006 amendment bill to include multiple devices in a named person warrant. The Department stated that this is evidenced by the then inclusion of sections 16 and 60(4)[42] which appear to recognise that additional devices can be added to a warrant.[43]

---

41 *Submission* 8, pp 3-4.

42 *Committee Hansard*, 17 April 2008, p. 29 and as quoted in *Submission* 1, p. 8.

43 *Committee Hansard*, 17 April 2008, p. 29. *Submission* 1, p. 8.

The inconsistencies between these provisions are described in detail in Chapter 2 of this report.

4.56 The Department informed the committee that the inconsistencies were the result of a drafting error that, 'did not allow for the original policy intention for various devices to be added to a warrant'.[44]

4.57 A representative of the NSW Council for Civil Liberties observed that a change 'that requires 12 changes in the Act and changes to six of its clauses… is not merely carrying out the intentions of an original amendment.'[45]

4.58 The submission by the Law Council also disputed the legislative intent of the provisions, drawing attention to the Government response to the committee's inquiry into the 2006 amendment Bill, which stated that:

> These warrants will only be issued where the requesting agency can show that the unique identifying number is indeed a unique source and there are no other practicable methods of identifying the service.[46]

Conclusion

4.59 The committee disagrees with the argument presented by the Department that the Bill merely 'clarifies' the intent of the Telecommunications (Interception) Amendment Bill 2006 that a device-based named person warrant gives the authority to intercept multiple devices.

4.60 The inclusion of the conflicting provisions (described above and in Chapter 2) in the TIA Act indicates that it may well have been the Department's intent to incorporate multiple device provisions, including the ability to add devices to the warrant after the issue of the warrant. However, this cannot necessarily be used as an indication of the Parliament's intent when it passed the legislation, and indeed there is evidence to the contrary view, including:

- the committee's report on the 2006 Bill, which made it clear that there were substantive concerns with the ability to uniquely identify a telecommunication device and that these concerns related to protection of individual privacy and rights;
- the government's response to the committee's 2006 report, which also clearly indicated that a device-based named person warrant required the device to be identified in the warrant; and
- service-based and device-based named person warrants are to be clearly differentiated in terms of the nature and extent of their powers, with devices

---

44 *Committee Hansard*, 17 April 2008, p. 29.

45 *Committee Hansard*, 17 April 2008, p. 8.

46 Australian Government response, quoted from *Submission* 1, p. 9.

> requiring greater safeguards. This is evidenced by the TIA Act requiring an issuing authority to be satisfied that there are no other practicable methods available at that time to identify—or it is impracticable to intercept—the telecommunications services that the person of interest is using, before issuing a device-based named person warrant.

4.61 Arguments about the intent of the legislation are, in any case, futile. It is not disputed that currently, the TIA Act does not allow for multiple devices on a device-based named person warrant, or for devices to be added after the warrant has been issued. The objective of this Bill is to enable these changes, and the purpose of this inquiry is to assess their effects and advise the Senate accordingly.

Suggestions for safeguards if devices are added to warrants

4.62 During the course of this inquiry, privacy and civil liberties groups all clearly agreed that an application for multiple devices, identified in a device-based named person warrant, is appropriate. The committee questioned witnesses who had raised other concerns in relation to the Bill's proposed amendments about whether agencies should be able to apply for a warrant for multiple devices. None objected to multiple devices being included in a single warrant application.[47]

4.63 The Castan Centre explained that this was not objectionable in principle as:

> Currently, to intercept a new device, the agency would have to get a new warrant. If that was rolled into a process whereby, under the one warrant application and issuing process, they could identify and make the case for interception of multiple devices, I think that would be unobjectionable. That would in effect just be combining multiple processes into one process. There would be no reason to think that would interfere with the oversight and accountability in respect of each of those devices named.[48]

4.64 However, these groups informed the committee that the existing safeguards for telecommunication devices, as currently required by the TIA Act, should be maintained if devices are subsequently added to a warrant. The Law Council submitted that maintaining the status quo requires an issuing authority to be satisfied that a person is a legitimate target of suspicion and:

> For each and every device that-
>
> - the interception is likely to yield useful information (unobtainable by other means);
> - the device is used or likely to be used by the suspect; and
> - the device can be uniquely identified.[49]

---

47 *Committee Hansard,* 17 April 2008, pp 4, 8, 12 and 22 and Law Council, answer to question on notice, 17 April 2008 (received on 24 April 2008). Note that EFA was not asked this question.

48 *Committee Hansard,* 17 April 2008, p. 4.

49 *Submission* 1, pp 5-7.

4.65 Scrutiny of these issues by an issuing authority would enable an authority to adequately test how much the privacy of any person or persons would be likely to be interfered with by intercepting under a warrant.

4.66 In a supplementary submission, the Privacy Foundation noted that its primary stance was to oppose a relaxation of the current issuing requirements for device-based warrants. However, the Privacy Foundation also put forward a model whereby an issuing authority would review additional devices within a short time-period, as follows:

> Agencies could be given an 'exceptional discretion' to intercept additional devices in relation to an existing named person warrant where timing or other operational circumstances made it impracticable to seek prior authorisation. However, exercise of this discretion would be subject to 'after the event' confirmation by an issuing authority, on presentation not only of the 'likely to be used' justification but also of the reasons for prior authorisation having been impracticable.
>
> Such an application for confirmation would be required within a fixed but short period after the interception of the additional device commenced. An issuing authority not persuaded by the case for the device could order immediate cessation of the interception….
>
> There is a clear precedent for this 'emergency authorisation' process in section 10 of the T(I&A) Act, which provides for the Director-General of Security to issue a warrant without the normal prior approval, subject to subsequent reporting to the Attorney-General and the Inspector-General.[50]

4.67 The Privacy Foundation also proposed a system of revocation and reprimand if the issuing authority was not persuaded by the case presented in the application for additional devices.

Proposed additional reporting of device-based warrant use

4.68 Part 2-8 of the TIA Act requires that the Attorney-General, as the Minister administering the TIA Act, prepare a report each year giving details of telecommunications interception for law enforcement purposes. The Department meets this requirement each year by publishing a consolidated report, the most recent of which is the *Telecommunications (Interception and Access) Act 1979, Annual Report for the year ending 30 June 2007.*

4.69 In relation to the need for additional safeguards if device-based warrant provisions are enacted, the Castan Centre's submission drew the committee's attention to the detail of current reporting requirements. These include, in relation to named person warrants issued during the year by each agency or authority, how many of those warrants involved the interception of:

- a single telecommunications service;

50 *Submission* 10a, p. 1.

- between two and five services;
- between six and ten services;
- more than ten telecommunications services; and
- the total number of telecommunication services intercepted under those warrants.

4.70 These requirements incorporate interceptions resulting from both device-based and service-based warrants, as the reporting is expressed in terms of the total number of services intercepted. There is no separate information provided in annual reports about the number or nature of devices intercepted.

4.71 The Castan Centre confirmed that the Bill is currently silent in terms of device-based reporting requirements and suggested that, were the proposed provisions for device-based warrants to be enacted, similar reporting to that in force for services should be required for device-based warrants, separately from service-based warrants. The Castan Centre argued that this would permit a degree of public scrutiny of the use to which the new power was being put.[51] Representatives of the Law Council supported the Castan Centre's view.[52]

4.72 EFA also supported the extension of reporting requirements to disaggregate device-based warrants. While considering this as a 'minimum', EFA argued that existing requirements are insufficiently detailed to allow scrutiny of the extent to which services additional to those identified in the original warrant application were intercepted. This point was illustrated in the following example:

> For example, one current reporting obligation is to report how many warrants 'involved the interception of more than 10 telecommunications services'. If a service-based named person warrant is issued, which identifies only one telecommunications service, and the agency involved intercepts a further 10 telecommunications services because they consider it 'likely' that the named person will use those services, would this warrant be reported as a warrant involving a single service, or more than 10 services?[53]

4.73 EFA submitted that there is a need for an additional reporting requirement to allow the disaggregation of services intercepted by services or devices identified in the original warrant, and those intercepted by services or devices subsequently added to the warrant. Additionally, this should be reported independently for service-based and device-based named person warrants. EFA considered that this is necessary because 'Statistics on this issue would indicate whether or not interception agencies might be overusing this power.'[54]

---

51 *Submission 8*, p. 7.

52 *Committee Hansard*, 17 April 2008, p. 12.

53 Answer to question on notice, 17 April 2008 (received on 22 April 2008), p. 1.

54 Answer to question on notice, 17 April 2008 (received on 22 April 2008), p. 1.

4.74 The committee sought a response from the representatives of the Department about the merits of this argument. Representatives confirmed that there is no additional reporting of the actual number of devices, but emphasised that the number of services intercepted under any device will still be reported in the annual report, as current reporting is on the number of services intercepted by all named person warrants:

> …regardless of the technology, whether it is done by device or service, it is the number of services that are intercepted that gives an indication of how many telecommunication services have been intercepted. The device is the technology by which the interception takes place.[55]

4.75 When asked to do so by the committee, the Departmental representative said that she was unable to comment on the merits of a specific reporting requirement for device based warrants, '…given that I believe the information is already in the reporting'.[56]

Balance of probabilities test

4.76 EFA submitted to the committee that the term 'likely' (as discussed in chapter 2, commencing at 2.16) was too open to interpretation in relation to a suspect 'using or likely to use' each device from which communications will be intercepted. The EFA stated:

> …the standard of a 'real chance or possibility' would be unacceptably low, and would both encourage and facilitate fishing expeditions by agencies with interception powers. These fishing expeditions could result in the interception of telecommunications devices belonging to a suspect's friends, relatives or workmates, not because the agency concerned believes that the suspect *will* use those devices, but merely because they *might*.[57]

4.77 A representative of the EFA told the committee that the word 'likely' is unclear, and is given various meanings by different courts, considering different legislation at different times. He said the meaning can range from the balance of probabilities, as in 'more likely than not', as a layperson would interpret it, to the low standard of a real chance or possibility. He stated that a balance of probabilities test is required.[58]

4.78 The committee asked the Department whether it would consider a balance of probabilities test. The Department's response was that it considered that the phrase 'likely to use' is an appropriate test:

---

55 *Committee Hansard*, 17 April 2008, p. 29.

56 *Committee Hansard*, 17 April 2008, p. 29.

57 *Submission*, p. 2.

58 *Committee Hansard*, 17 April 2008, p. 18.

> The 'likely to use expression in section 46A provides a mechanism that enables intelligence gathering where something is likely to occur in the future. Human action is difficult to predict. However, in the context of the TIA Act, the term 'likely' should be interpreted as being analogous with a 'real risk'[59] or 'probable[60] that the named person is using or likely to use a device. To satisfy such a test would require evidence as to why an agency suspects that a person is likely to use a device.[61]

Discarding of data from persons not named in the warrant

4.79 On being questioned by the committee on additional safeguards that would limit surveillance of non-suspects in device-based warrants, a representative of EFA suggested that it could be a requirement that all communications that were not made by the person named in the warrant be discarded. The representative went on to state that it was EFA's understanding that:

> … under the law as it currently stands, the communications of those persons can be recorded and are only discarded if they are not really relevant to a crime which is investigated by that type of agency….It says on page 4 of the A-G's [Attorney General's] submission:
>
> - Intercepted material must be destroyed where it is not relevant to the permitted purposes of the agency—generally an investigation of an offence that is punishable by three years imprisonment or more.[62]

4.80 A representative of the Department responded to the committee's questions on the secondary use of data stating that there are no legislative provisions relating to the collection of interception data for general intelligence, no centralised database for its storage and that it is an offence to disclose intercepted information, except for the permitted purposes for which it is obtained. The representative stated that:

> There is no derivative use of TI [telecommunications interception] product except for those very limited grounds which are in the Act, and that is for the permitted purpose of the original investigation or to pass it over for a relevant offence, which has to be punishable by at least three years imprisonment. So it is very, very tightly guarded. Certainly the AFP can talk more about their destruction provisions, but each intercepting agency has very strong accountability regimes inside such that they do have to destroy, and it is part of the role of those oversight bodies like the Ombudsman that they review and make sure that that has actually been

---

59 Secretary, Department of Employment, Education, Training Youth Affairs v Suzanne Barrett & Anor (1998) 82 FCR 524, in Attorney General's Department, answer to question on notice, 17 April 2008 (received on 24 April 2008), p. 1.

60 Australian Telecommunications Commission v Krieg Enterprises Pty Ltd (1976) 14 SASR 303 at 309-313, in Attorney General's Department, answer to question on notice, 17 April 2008 (received on 24 April 2008), p. 1.

61 Answer to question on notice, 17 April 2008 (received on 24 April 2008), p. 1.

62 *Committee Hansard*, 17 April 2008, p. 19.

> undertaken. And, if not, then reports are made to ministers that they have breached their obligations to destroy particular information.[63]

4.81 The committee notes that the offence threshold for the secondary use of data appears to be less restrictive, than that which applies when an issuing authority considers a device-based named person warrant application. For example, the Department's submission stated that an issuing authority for such a warrant would need to be satisfied that:

> … the interception is for an investigation of a serious offence, generally punishable by a maximum period of imprisonment of at least seven years.[64]

Committee findings

4.82 The committee considers it desirable that an issuing authority should be able to approve multiple devices identified in a device-based named person warrant application and add additional identified devices to that warrant at later stages.

4.83 The committee considers that the process of adding a device to a device-based named person warrant after the warrant has been issued should include an independent scrutiny process. The committee considers that the model proposed by the Australian Privacy Foundation, discussed at paragraph 4.66, provides a useful starting point.

4.84 The committee considers that the annual report on the TIA Act is reasonably comprehensive in terms of providing a breakdown of interceptions that have taken place and the agencies undertaking the interceptions. However, it is also important for the Parliament to be able to discern the effects of any new legislation and accordingly, the committee is of the view that additional reporting of the use of these powers is required.

4.85 The committee considers that the number of services intercepted by service-based and device-based named person warrants should be disaggregated, and the results presented in a similar manner to that currently for intercepted services. The committee also considers that the number of services intercepted pursuant to the services or devices in the original application should be reported separately to the services intercepted by later additions to the warrant. This should be reported separately for device-based and service based named person warrants in a similar manner to that currently used for the reporting of intercepted services.

---

63 *Committee Hansard*, 17 April 2008, p. 30.

64 *Submission* 7, p. 3.

Recommendation 2

4.86 The committee recommends that the recommendation at paragraph 3.2.5 of the Blunn report, which reads:

> **3.2.5. Accordingly, I recommend that priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.**

be adopted, and priority given to developing a unique and indelible identifier of the source of telecommunications.

Recommendation 3

4.87 The committee recommends that the Bill be amended to provide that an agency be permitted to add a device to a device-based named person warrant after the warrant has been issued if the facts of the case would have justified the issue of a warrant by the issuing authority; and the investigation in relation to the person named in the warrant will be, or is likely to be, seriously prejudiced if the interception does not proceed.

Recommendation 4

4.88 The committee further recommends that the Bill be amended to provide that if an agency adds a telecommunications device or devices not identified on a device-based named person warrant at the time that the issuing authority issued the warrant:

(i) the agency be required to notify an issuing authority, within 2 working days, that a device had been added to the warrant; and

(ii) the issuing authority must examine the supporting documentation against the criteria that it would have considered, in accordance with the requirements of the *Telecommunications (Interception and Access) Act 1979*, in relation to an application by the agency for a device-based named person warrant, and make a determination about whether the facts of the case justified the addition of the device; and

(iii) the issuing authority shall order that the interception cease immediately and that all evidence gathered be destroyed if it determines that the facts of the case would not have supported the issue of a device-based named person warrant.

Recommendation 5

4.89 The committee recommends that the Bill be amended to insert a requirement that the Annual Report in relation to the *Telecommunications (Interception and Access) Act 1979* incorporate the following additional information over and above that already required by the Act:

- **the number of service-based and device-based interceptions, to be reported upon separately but in a similar format to that currently used for the total number of intercepted telecommunication services; and**

- **the number of devices in the original warrant and the number of additional devices added to the warrant, reported in a similar format to that currently used for reporting the total number of intercepted telecommunications services.**

CHAPTER 5

NOTIFICATIONS TO AND FROM STATE MINISTERS

Concerns about the proposal

5.1 A number of submitters to the inquiry expressed disquiet about the proposed removal of the requirement in the TIA Act for state agencies to provide a copy of each warrant and instrument of revocation to the responsible state minister. Several witnesses expressed concern that removing the requirement for state agencies to provide copies of warrants to state ministers represented a lessening of accountability safeguards that currently apply to the warrants process; a shifting of responsibility to the Commonwealth Attorney-General's Department; and may possibly lead to agencies acting outside of their current legislative requirements.

5.2 The Victorian Privacy Commissioner disagreed with the removal of the mandatory requirements for state interception agencies to report to state ministers, noting that the approach of state ministers to warrants may differ from that of the Commonwealth Attorney-General. The Commissioner said that this is particularly so in jurisdictions like Victoria, which has a Charter of Human Rights and Responsibilities with which all state agencies, including law enforcement agencies, are required to comply. The Commissioner concluded that the existing mandatory reporting provides a better safeguard and should be maintained.[1]

5.3 The Australian Privacy Foundation (Privacy Foundation) also opposed the removal of the mandatory requirement. The Privacy Foundation noted that the change was ostensibly to 'avoid duplication', but questioned whether it was desirable to:

> …cut the State governments out of the routine reporting loop in the way proposed. Keeping State Ministers informed of warrants is a useful safeguard-they may question them when the Commonwealth Attorney would not. No information has been provided about the views of the States on this change. The provision for 'optional' State reporting doesn't necessarily address the issue – State governments may well not take the trouble to 'opt-in' and then quietly forget all about the interception being done by their agencies-there is merit in our view having them 'force fed' the warrant information. While this cannot ensure that they apply an appropriate degree of scrutiny, the potential for them to do so is another important safeguard.[2]

5.4 At the hearing, a representative of the Privacy Foundation explained that when copies of warrants are provided to state ministers, this opens up an opportunity

---

1 *Submission* 5, p. 2.

2 Australian Privacy Foundation, *Submission* 10, p. 2.

for a second person to potentially observe any patterns of use that may be of concern; and that this was a safeguard that the Privacy Foundation would be loath to lose:

> If it is all entirely left to the federal Attorney-General, you only have one watchdog. In our view, it is more important to have two watchdogs that, whilst they might not bite very often, at least occasionally might be awake.[3]

5.5 The committee questioned representatives of the Attorney-General's Department about whether removing the requirement for state ministers to receive copies of warrants would somehow lessen their accountability or responsibility for the activities of their agencies. Representatives disagreed with this proposition, stating that the oversight activities of the ombudsmen in each state addressed this potential problem:

> There is the oversight requirement that ombudsmen or like agencies in the states have to undertake a review of the interception reporting requirements and accountability reports are made to each state minister by those particular oversight authorities which actually give them details of the activity that has been undertaken by the agencies within their jurisdiction. That is a much more meaningful report than receiving a copy of a warrant in a bundle with others, which is then passed on to a Commonwealth minister.[4]

Committee findings

5.6 The committee notes that the proposal in the Bill is apparently consistent with aspects of the Blunn review and Mr Blunn's observations that there is little purpose in a state minister acting merely as a conduit between the state agencies and the Commonwealth Attorney-General.

5.7 However, as described in Chapter 2 of this report, Mr Blunn also raised concerns about whether the minister was meeting the intention of the TIA Act by relying on reports of the Ombudsman, a concern that the committee shares.

5.8 It is difficult for the committee to form a view about this issue in the absence of more detailed information. As a matter of principle, the committee shares the view of Mr Blunn that responsibility for the actions of state agencies must ultimately rest with their ministers:

> There should be no suggestion that the agencies are reporting directly to the Attorney-General who is then responsible for their actions. In my opinion that responsibility must rest with the State Minister.[5]

---

3 *Committee Hansard,* 17 April 2008, p. 25

4 *Committee Hansard*, 17 April 2008, pp 28-29.

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

CHAPTER 6

OTHER ISSUES

International, national and state obligations

6.1 The Castan Centre for Human Rights Law (Castan Centre) submitted that 'in the absence of an express right to privacy under Australian Law, legislation such as the TIA Act plays an important role in safeguarding the privacy of individuals'.[1] In particular, their submission stated that Australia should ensure it meets its international obligations under Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which states that:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

6.2 A representative of the NSW Council for Civil Liberties stated that the proposed amendments for device-based warrants constitute 'an arbitrary interference with the right of privacy' in contravention of obligations such as the ICCPR. The representative also considered that the proposed amendments would contravene various state and territory legislation for example, the *Charter of Human Rights and Responsibilities Act 2006* (Vic), and the *Human Rights Act 2004* (ACT)[2]. The representative said that these obligations and legislation enshrine a right to privacy, and that:

> One would (expect to) find that this committee would have before it a statement of compatibility, prepared by the minister introducing this bill, as to the compatibility or non-compatibility of the provisions of the bill with that privacy right.[3]

6.3 The Committee also sought information from representatives of the Attorney-General's Department about interception standards in any United Kingdom legislation comparable to the TIA Act. The Department's response was that the provisions most likely to be related to the addition of devices in a warrant were governed by the *Regulation of Investigatory Powers Act 2000* (RIPA). The Department stated:

> …RIPA makes provision for and about the interception of communications, the acquisition and disclosure of data relating to communications, as well as other investigatory techniques. An important difference between RIPA and the Australian *Telecommunications (Interception and Access) Act 1979* (the TIA Act) is that the UK regime is non-evidentiary based. As the intercepted material is not used in evidence, RIPA has different approaches to the

---

1 *Submission* 1, p. 4.

2 Respectively, this refers to section 13 and 12 of the Acts.

3 *Committee Hansard*, 17 April 2008, p. 7.

> collection of information, use and disclosure, and record keeping requirements.[4]

6.4 The Department further stated that the RIPA equivalent of device-based named person warrants in the TIA Act must describe either.

> (a) one person as the interception subject; or
>
> (b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place. [And]
>
> (2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.[5]

6.5 The Department advised that the RIPA allows the addition of devices to an existing warrant, which does not extend the original duration of the warrant. A description of the approval authorities followed:

> Whilst only a Secretary of State is authorised to issue a warrant, scheduled parts of a warrant may be modified by a Secretary of State or by a senior official acting upon their behalf (this, except in urgent cases, does not include the senior official who made the warrant application). A senior official is defined in subsection 81(1) of RIPA as a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service. These designations are equivalent to the Australian Senior Executive Service and represents a similar proportion of the entire Civil Service/Public Service workforce.
>
> … In urgent cases, and where the warrant specifically authorises it, the person who submitted the application (…they are listed in subsection 6(2) and are Heads of Agencies, ie Director-General of the Security Service, the Commissioner of Police of the Metropolis etc) or a subordinate (where identified in the warant) may modify scheduled parts of the warrant. These modifications are valid for five working days only unless endorsed by a senior official acting on behalf of the Secretary of State.[6]

Five year review of the TIA Act

6.6 In its submission to the committee, the Office of the Privacy Commissioner (OPC) reiterated its view that the operation of the TIA Act 'should be subject to overall independent review at least every five years.'[7] The OPC considered this necessary due to the number of amendments to interception legislation in recent years and the resulting incremental expansion in powers.

---

4 Attorney-General's Department: answers to questions on notice, received 24 April 2008

5 Attorney-General's Department: answers to questions on notice, received 24 April 2008

6 Attorney-General's Department: answers to questions on notice, received 24 April 2008.

7 *Submission* 7, p. 9.

6.7 The OPC also submitted a framework against which to assess issues such as privacy and security. The OPC recommended that the committee consider the amendments in the Bill against this framework because of the incremental expansion of powers and suggested that it may also be a useful tool for interception agencies to use.[8]

Committee findings

6.8 In relation to international obligations and state legislation, the committee is unable to make any specific comments in the context of the current inquiry. Nevertheless, in development of amendments to interception legislation and in any review of that legislation, due consideration of the international obligations must be undertaken. A summary statement in the EM of consistency with international obligations (in lieu of an express right to privacy under Australian law) would be a useful guide in consideration of future legislative amendments.

6.9 In relation to the five year review process proposed by the Office of the Privacy Commissioner, the committee draws the attention of the Senate to recommendation 4 of the committee's report on the TIA Amendment Bill 2007, proposing an independent review of the TIA Act within five years.[9] There has been no government response to this recommendation.

6.10 The committee also reminds the Senate of its recommendation in its report in relation to the Provisions of the Telecommunications (Interception) Amendment Bill 2006:

> …the Bill should include a provision for the provisions to expire in five years, with a review at that time or earlier. The Review should encompass the broader issues surrounding the suitability and effectiveness of AAT members in the warrant issuing regime, together with consideration of ways in which the Act may be amended to take account of emerging technologies such as peer-to-peer technology.

6.11 The Howard Government did not accept this recommendation stating:

> Where it was considered appropriate, sunset provisions have been included for specific provisions in the Bill….
>
> However, the Government does not consider a sunset clause to be appropriate in relation to the wider Bill. The matters proposed in this bill do not reflect a response to a particular short term issue that is likely to dissipate in the longer term. Rather, this legislation reflects a response to permanent changes in the law enforcement and national security environment, caused in large part by changes in technology. As such, it is anticipated that these legislative provisions will assume even greater importance in future.

---

8 *Submission* 7, p. 2.

9 Telecommunications (Interception and Access) Amendment Bill 2007, p. 48.

6.12 In this context, the committee notes that it is currently considering amendments to the device-based warrant regime which was enacted in 2006. It also notes that several of the issues which raised concerns in both the 2006 and 2007 bills have re-emerged in the context of the current inquiry.

Recommendation 6

6.13 **The Committee recommends that the Australian Government commission an independent review of the operation of the *Telecommunications (Interception and Access) Act 1979* within 3 years.**

Recommendation 7

6.14 **The Committee further recommends that the Australian Government introduce amendments to the *Telecommunications (Interception and Access) Act 1979* in subsequent legislation, to provide for a statutory requirement that the TIA Act be independently reviewed every five years.**

Recommendation 8

6.15 **Subject to the preceding recommendations the committee recommends that the Senate pass the Bill.**

Senator Trish Crossin

Chair

SUPPLEMENTARY REPORT WITH ADDITIONAL COMMENTS OF DISSENT BY THE AUSTRALIAN DEMOCRATS

1.1 The Democrats commend the Chair and Committee Secretariat on the comprehensive and considered nature of the Committee's report and agree with the majority of the Committee's recommendations.

1.2 We believe that the recommendations made by the Committee will provide additional privacy protections and improve the overall accountability of the telecommunications interception regime.

1.3 However, the Democrats have a number of additional concerns which we consider should be addressed before the bill is passed.

The Government's attitude to legislation affecting national security

1.4 The Government contends that the main purpose of this bill is to amend the TIA Act to extend by eighteen months the operation of the network protection provisions which are due to sunset on 13 June 2008. For this reason, Parliament was asked to consider the bill time critical and the Government initially sought to have it included in the non-controversial legislation list.

1.5 It was asserted in the Attorney-General's second reading speech that the remainder of the bill implements a number of 'minor yet important technical amendments', and that the bill 'contains no new powers for security or law enforcement agencies in relation to telecommunications interception, stored communications or access to data, but ensures that these agencies have the necessary tools to combat crime in this age of rapid technological change'.

1.6 It is of great concern to the Democrats that on the first occasion that the new Government turns its mind to any form of legislation that impacts upon Australia's national security regime, it has labelled the bill 'time critical' and sought to limit debate.

1.7 Indeed, during a detailed debate on the 2006 amendment bill which carried over three days in the Senate Chamber, the then Opposition moved a series of amendments to the TIA Act. The amendments focussed on the then Opposition's concern that the legislation did not adequately protect individual privacy, particularly in relation to B-Party warrants

1.8 Senator Ludwig, the then Shadow Minister for Justice and Customs and Manager of Opposition Business in the Senate, carried the debate. During the third reading speech, Senator Ludwig said:

> *'The position we have now got to is that the government has voted down sensible amendments which came out of the committee process…..It is unfortunate that this government has not picked up the amendments that Labor has proposed, safeguards*

which would have struck the right balance. It really comes down to a lazy Attorney-General, who has not had the opportunity to look at the recommendations, to bring forward amendments and to argue for them in here. That is why this extended process has occurred: because of a lazy Attorney-General. There is no other way of putting it.

The government could have picked up our recommendations during this debate. They have not. Therefore, they have not struck the right balance. Privacy is not sufficiently protected so far as B-party intercept warrants are concerned.'[1]

1.9 However, in one of its first legislative acts in the new Parliament, the Government has revisited this legislation, attempted to curtail debate, and has made no attempt to address the numerous concerns that it had with the legislation in 2006.

1.10 Further, it is clear from the nature and extent of submissions received to this inquiry and from the detailed consideration and conclusions contained in the Chair's report, that the amendments proposed by this bill are far from 'minor' or 'technical'. Indeed, the Chair has concluded (at paragraph 4.30) that the amendments in relation device-based warrants 'propose to remove an important existing safeguard'.

1.11 The Democrats also recommended a series of amendments to the TIA Act when the 2006 amendment bill was passed, particularly in relation to B-party warrants, and recommended further amendments when the 2007 amendment bill was before the Senate, particularly in relation to warrantless access to prospective or 'real time' telecommunications data.

1.12 In the circumstances, the Democrats consider that the TIA Act requires significant further amendment in areas which have not been addressed by this bill.

Recommendation 1

The Democrats recommend that the Government immediately review the privacy protections available under the TIA Act with a view to implementing amendments moved by the then Opposition and the Australian Democrats when the TIA Act was amended in 2006 and 2007.

Extension of the sunset provisions

1.13 The Democrats agree with the Chair's conclusion that the extension of the sunset provisions under subsections 5F(2) and 5G(2) of the TIA Act should be allowed to pass without amendment.

1.14 The Democrats also support the Chair's recommendation that any further legislation to address network protection provisions should include a thorough and considered response to achieving a balance between individual privacy rights and network protection requirements.

[1] *Senate Hansard*, Thursday, 30 March 2006, p.59.

1.15 However, the Democrats are concerned that progress in relation to a permanent legislative solution has not progressed beyond a draft discussion paper that has not been circulated outside the Attorney-General's Department[2].

1.16 The Democrats consider that such progress is unacceptably slow and urge the Government to work towards a permanent solution to this issue as expeditiously as possible.

1.17 The Democrats also note the there is a degree of uncertainly surrounding the application of the TIA Act to organisations other than law enforcement and intelligence agencies that do not have the benefit of an exemption.

1.18 As Electronic Frontiers Australia stated during this inquiry:

> *'Simply put, it seems now that ASIO, the police and anticorruption agencies may be able to legally filter viruses and spam from their incoming email but there is a good chance that organisations in the private sector and indeed government organisations not specifically provided for in the legislation may be committing an offence by doing that.'*[3]

1.19 The Democrats note recent comments from the Attorney-General that indicate that the Department is developing a solution to this problem.

1.20 The Democrats consider that any uncertainty surrounding the application of the TIA Act to non-exempt organisations should be addressed as a matter of urgency and, if clarifying legislation is required, it should be developed commensurate with the permanent legislative solution in respect of law enforcement and intelligence agencies.

Recommendation 2

> **The Democrats recommend that the Government develop a permanent legislative solution in relation to the monitoring of electronic communications by both Government and non-Government organisations as a matter of urgency.**

Device-based named person warrants

1.21 Device based interception warrants were introduced by the 2006 amendment bill.

1.22 During the Committee inquiry into the 2006 amendment bill, the Democrats considered that there was significant uncertainty surrounding the ability to uniquely identify communications devices and recommended that the provisions of the 2006

---

[2] *Committee Hansard*, Thursday, 17 April 2008, p.28.

[3] *Committee Hansard*, Thursday, 17 April 2008, p.16.

amendment bill relating to device based warrants be delayed until it was possible to determine the full scope of their operation[4].

1.23 The Democrats note the concern expressed by privacy and civil liberties groups, as reflected in the Chair's report, regarding the continued uncertainty in relation to unique identifiers.

1.24 Accordingly, the Democrats support the Committee's recommendation to implement recommendation 3.2.5 of the Blunn report and that and priority given to developing a unique and indelible identifier of the source of telecommunications.

1.25 However, the Democrats consider that the implementation of recommendation 3.2.5 of the Blunn report should be a condition precedent to access to telecommunications via devoice-based warrants.

1.26 The Blunn report did not recommend the introduction of device-based warrants, rather 'that priority be given to developing a unique and indelible identifier of the source of telecommunications **and therefore as a basis for access**' (emphasis added).

1.27 The Democrats consider that to allow the development and expansion of the device-based warrant regime before the development of a 'unique and indelible identifier' is to 'put the cart before the horse'. We consider that the risk posed by inadvertent privacy invasion due to inaccurate or incorrect device identification is too high.

1.28 Accordingly, the Democrats consider that the provisions in the bill in relation to device based warrants should be deleted.

1.29 Notwithstanding, while the Democrats maintain an in-principle objection to the expansion of the device-based warrant regime, we support the Committee's conclusions (at 4.48 to 4.50) that:

- 'after the fact' reporting is insufficient to adequately assess issues associated with individuals' privacy and rights; and
- internal accountability mechanism are unacceptable and the best practice is to maintain independent scrutiny, should agencies be authorised to add devices to a warrant, except in exceptional circumstances.

1.30 We consider that the Committee recommendations numbers 3, 4 and 5 in Chapter 4 will improve the bill immeasurably by creating a more transparent and independent authorisation mechanism for device-based warrants.

1.31 If the Senate considers it appropriate to proceed in line with these recommendations, the Democrats consider that an appropriate addition to recommendation 4 would provide that, where an issuing authority determines that a

[4] Committee report on the provisions of the *Telecommunications(Interception and Access) Amendment Bill 2006*, p. 65.

person has been subject to unlawful interception, that person shall be notified of the interception immediately unless such notification would materially prejudice the conduct of an ongoing investigation.

1.32 The Democrats also reserve the right to move additional amendments subject to the final form of the bill when it is debated in the Senate.

Recommendation 3

> **The Democrats recommend that the provisions in the Bill in relation to device-based named person warrants should be deleted.**

Recommendation 4

> **The Democrats recommend that, if the provisions in the Bill in relation to device-based named person warrants are passed with a requirement for independent examination by an issuing authority and the authority determines that the addition of devices to an existing warrant was unlawful, the person subject to the unlawful interception should be notified of the interception immediately unless such notification would materially prejudice the conduct of an ongoing investigation.**

International, national and state obligations

1.33 The Democrats support the Committee's recommendations that the Government commission an independent review of the operation of the TIA within three years; and that the TIA Act be amended to provide a statutory requirement for independent review every five years.

1.34 The Democrats also support the Committee's conclusion that a summary statement in the EM of consistency with international obligations (in lieu of an express right to privacy under Australian law) would be a useful guide when considering any further legislative amendments.

Public Interest Monitor

1.35 The Democrats view this Bill as an expansion of the telecommunications monitoring powers of the Commonwealth. The Democrats also consider that the significant other amendments made to the TIA Act during 2006 and 2007 did not adequately address privacy concerns.

1.36 As a result, there is a significant risk that the powers available to law enforcement and security agencies under the TIA Act could breach the privacy rights of Australian citizens.

1.37 As such it is appropriate that there be an independent umpire to balance necessary, lawful, and proportionate access by law enforcement agencies to telecommunications data with the public's right to communicate free from surveillance.

1.38 The Democrats note that in relation to the area of listening devices, a model can be found in Queensland, where a Public Interest Monitor is authorised under the *Police Powers and Responsibilities Act 2000* (Qld) to intervene in applications for listening devices warrants, and to monitor and report on the use and effectiveness of the warrants.

1.39 The Democrats see merit in adopting the Queensland public interest monitor model to improve accountability.

Recommendation 5

> **The Democrats recommend that the TIA Act be amended to require law enforcement and intelligence agencies to consult with a Public Interest Monitor (PIM) before they apply for an authorisation under the TIA Act.**

Senator Natasha Stott Despoja

Australian Democrats

APPENDIX 1

SUBMISSIONS AND ADDITIONAL INFORMATION RECEIVED

Submission Number	Submittor
1.	Law Council of Australia
2.	NSW Council for Civil Liberties
3.	Office of NSW Privacy Commissioner
4.	Attorney-General's Department
5.	Victorian Privacy Commissioner
6.	Australian Security Intelligence Organisation (confidential submission)
7.	Office of the Privacy Commissioner
8.	Castan Centre for Human Rights Law
9.	Victorian Police
10.	Australian Privacy Foundation
10a.	Australian Privacy Foundation – supplementary submission
11.	Electronic Frontiers Australia
12.	Australian Federal Police
13.	Tasmanian Police
14.	Queensland Police

ADDITIONAL INFORMATION RECEIVED

1. Answers to Questions on Notice received from Electronic Frontiers Australia
2. Answers to Questions on Notice received from the Law Council of Australia
3. Answers to Questions on Notice received from the Attorney-General's Department

APPENDIX 2

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

Sydney, Thursday 17 April 2008

BIBBY, Dr Richard Martin, Convenor, Civil and Indigenous Rights Subcommittee
New South Wales Council for Civil Liberties

BLANKS, Mr Stephen, Secretary
New South Wales Council for Civil Liberties

CLAPPERTON, Mr Dale, Chair
Electronic Frontiers Australia

EMERTON, Dr Patrick, Castan Centre Associate
Castan Centre for Human Rights Law, Monash University

KELLY, Ms Wendy, Acting Director, Telecommunications and Surveillance Law Branch
Attorney-General's Department

MOULDS, Ms Sarah, Policy Lawyer
Law Council of Australia

SMITH, Ms Catherine, Assistant Secretary, Telecommunications and Surveillance Law Branch
Attorney-General's Department

WATERS, Mr Nigel, Board Member
Australian Privacy Foundation

WHOWELL, Mr Peter, Manager, Legislation Program
Australian Federal Police

WILSON, Mr Ian, Manager, Business and Technical Delivery, High Tech Crime Operations
Australian Federal Police