The Senate

Standing Committee on Legal and Constitutional Affairs

Telecommunications (Interception and Access) Amendment Bill 2007 [Provisions]

August 2007

ISBN: 978-0-642-71832-7

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

MEMBERS OF THE COMMITTEE

Members
Senator Guy Barnett, **Chair**, LP, TAS
Senator Patricia Crossin, **Deputy Chair**, ALP, NT
Senator Andrew Bartlett, AD, QLD
Senator Marise Payne, LP, NSW
Senator Stephen Parry, LP, TAS
Senator Linda Kirk, ALP, SA
Senator Joe Ludwig, ALP, QLD
Senator Russell Trood, LP, QLD

Participating Member
Senator Natasha Stott Despoja, SA, AD

Secretariat

Ms Jackie Morris	Secretary
Ms Sue Harris Rimmer	Principal Research Officer
Ms Judith Wuest	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

MEMBERS OF THE COMMITTEE **iii**
ABBREVIATIONS **vii**
RECOMMENDATIONS **ix**

CHAPTER 1 **1**
INTRODUCTION **1**
Purpose of the Bill 1
Background 1
Conduct of the inquiry 2
Acknowledgement 2
Note on references 2

CHAPTER 2 **3**
OVERVIEW OF THE BILL **3**
Current regime 3
Legislative history 4
Summary of provisions 7

CHAPTER 3 **15**
KEY ISSUES **15**
Consultation 15
Definitions 16
Privacy concerns 21
Obligations on carriers and carriage service providers 26
Other issues 32
Committee view 34

MINORITY REPORT BY THE AUSTRALIAN DEMOCRATS **37**

APPENDIX 1 **43**
Submission and additional information received

APPENDIX 2 **45**
Witnesses who appeared before the committee

ABBREVIATIONS

AAT	Administrative Appeals Tribunal
ACMA	Australian Communications and Media Authority
AFP	Australian Federal Police
AMTA	Australian Mobile Telecommunications Association
Annual Report	*Telecommunications (Interception and Access) Act 1979 Report for the year ending 30 June 2006*
APF	Australian Privacy Foundation
ASIO	Australian Security Intelligence Organisation
the Bill	Telecommunications (Interception and Access) Amendment Bill 2007
Blunn Review	*Review of the Regulation of Access to Communications* by Anthony Blunn AO, August 2005
CAC	Communications Access Coordinator
CCR	Call Charge Records
CSP	Carriage Service Provider
Department	Attorney-General's Department
EFA	Electronic Frontiers Australia
EM	Explanatory Memorandum
ICP	Interception Capability Plan/s
IGIS	Inspector-General of Intelligence and Security
Law Council	Law Council of Australia
OPC	Office of the Privacy Commissioner
Police Federation of Australia	Police Federation
Telecommunications Act	*Telecommunications Act 1997*
TIA Act	*Telecommunications (Interception and Access) Act 1979)*

RECOMMENDATIONS

Recommendation 1

3.77 The committee recommends that proposed paragraph 5(1)(m) of the Bill be deleted to remove CrimTrac from the definition of 'enforcement agency'.

Recommendation 2

3.78 The committee recommends that the determination of the Communications Access Coordinator under proposed subsection 183(2) address requirements for the consideration and documentation of privacy issues by authorised officers.

Recommendation 3

3.79 The committee recommends that the Inspector-General of Intelligence and Security incorporate into his regular inspection program oversight of the use of powers to obtain prospective telecommunications data by the Australian Security Intelligence Organisation.

Recommendation 4

3.80 The committee recommends that the Attorney-General's Department arrange for an independent review of the operation of the *Telecommunications (Interception and Access) Act 1979* within five years.

Recommendation 5

3.81 Subject to the preceding recommendations, the committee recommends that the Bill be passed.

CHAPTER 1

INTRODUCTION

Purpose of the Bill

1.1 On 21 June 2007, the Senate referred the provisions of the Telecommunications (Interception and Access) Amendment Bill 2007 (the Bill) to the Legal and Constitutional Affairs Committee for inquiry and report by 1 August 2007.

1.2 The Bill amends the *Telecommunications (Interception and Access) Act 1979* (the TIA Act)[1] and several other related Acts to implement further recommendations from the August 2005 *Review of the Regulation of Access to Communications* by Anthony Blunn AO (the Blunn Review).

1.3 The main purpose of the Bill is to transfer the national security and law enforcement-related provisions from the *Telecommunications Act 1997* (the Telecommunications Act) to the TIA Act. This would complete the development of a single legislative framework for national security and law enforcement agencies to access telecommunications-related data as envisaged by the Blunn Review.

1.4 The Bill also contains a number of additional amendments to the operation of the existing TIA Act.

1.5 An Exposure Draft of the Bill was advertised by the Telecommunications Interception and Surveillance section of the Attorney-General's Department (the Department) in January 2007. The Department website details a consultation process beginning in early February 2007, involving the telecommunications industry, law enforcement and national security agencies, which precipitated a number of changes to the Exposure Draft.

Background

1.6 The Blunn Review recommended that comprehensive and over-riding legislation dealing with access to telecommunications data for security and law enforcement purposes be established.

1.7 The first tranche of Blunn Review amendments contained certain measures, such as stored communication warrants and B Party intercepts, which have already become law. The *Telecommunications (Interception) Amendment Act 2006* received Royal Assent on 3 May 2006.

---

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

Conduct of the inquiry

1.8 The committee advertised the inquiry in *The Australian* newspaper on 27 June 2007 and 11 July 2007, and invited submissions by 11 July 2007. Details of the inquiry, the Bill, and associated documents were placed on the committee's website. The committee also wrote to over 80 organisations and individuals.

1.9 The committee received 27 submissions which are listed at Appendix 1. With the exception of one confidential submission, submissions were placed on the committee's website for ease of access by the public.

1.10 The committee held a public hearing in Canberra on 16 July 2007. A list of witnesses who appeared at the hearing is at Appendix 2 and copies of the Hansard transcript are available through the Internet at http://aph.gov.au/hansard.

Acknowledgement

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

Note on references

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

CHAPTER 2

OVERVIEW OF THE BILL

2.1 This chapter briefly outlines the main provisions of the Bill.

Current regime

2.2 The TIA Act has two main objectives. Its primary object is to protect the privacy of individuals who use the Australian telecommunications system by making it an offence to intercept communications passing over that system, or to access stored communications that have passed over that system, other than in accordance with the provisions of the TIA Act (sections 7 and 108). The second purpose of the TIA Act is to specify the circumstances in which it is lawful for the interception of, and access to, communications to take place.

2.3 There is currently a two tier hierarchy of interceptions made under warrants. A telecommunications service (such as a phone call) may be intercepted under the authority of a telecommunications interception warrant by an interception agency for the investigation of a serious offence (Part 2.5), or by the Australian Security Intelligence Organisation (ASIO) for national security purposes (Part 2.2). A stored communication (such as voicemail, email and SMS) may be accessed under the authority of a stored communications warrant by a law enforcement agency for the investigation of a serious contravention (Part 3.3), or by ASIO for national security purposes (Part 3.2).[1]

2.4 An overview of the current regime and lists of interception and law enforcement agencies can be found in the *Telecommunications (Interception and Access) Act 1979 Report for the year ending 30 June 2006* (the Annual Report).[2]

2.5 The Annual Report states the agency position on the utility of interception powers:

> There remains a consistent view among agencies that telecommunications interception continues to be an extremely valuable investigative tool. Agencies have again noted that evidence gathered through the execution of a telecommunications interception warrant can lead to the successful

---

1 The Department has set out the regime diagrammatically in a TIA Act table: see Additional Information No. 2, Diagrams tabled by Attorney-General's Department, Telecommunications and Surveillance Law Branch at the public hearing held in Canberra on Monday 16 July 2007, available from the committee's website.

2 Attorney-General's Department, *Telecommunications (Interception and Access) Act 1979 Report for the year ending 30 June 2006*, May 2007, at http://www.ag.gov.au/www/agd/agd.nsf/Page/Publications_Telecommunications(InterceptionandAccess)Act1979Reportfortheyearending30June2006 (accessed 1 July 2007).

> conclusion of an investigation in circumstances where alternative evidence is uncorroborated, unavailable or insubstantial.[3]

2.6 The Attorney-General also issued a press release on 9 May 2007 stating that telecommunications interception is a valuable aid to prosecuting crime:

> Telecommunications interception is an essential investigative tool which allows law enforcement agencies to identify and target persons involved in serious criminal activity.
>
> During the 12-month reporting period, almost 1500 convictions were secured with the assistance of intercepted communications.
>
> Over the same time, intercepted communications also supported more than 2000 arrests and the progression of more than 3000 prosecutions. Many of these ongoing prosecutions represent the culmination of investigations that have spanned a number of years.[4]

2.7 In recent articles, academics Bronitt and Stellios identified a steady increase in the issue of federal wiretap warrants[5] and stated that the legislative framework governing electronic surveillance is failing to keep up with technological advances and 'resembles a patchwork'.[6] They contested the 'balance' approach to regulation of telecommunications interception and argue that this approach sets up privacy rights and fighting serious crime as competing interests. Privacy or due process issues tend to consistently lose in this competition depending on how serious the crime is considered to be.[7]

Legislative history

2.8 The Blunn Review recommended that comprehensive and over-riding legislation dealing with access to telecommunications data for security and law enforcement purposes be established.[8]

---

3 p. 13.

4 The Hon. Mr Philip Ruddock MP, Attorney-General, 'Telecommunications Interception Aids Prosecution', *Media Release 088/2007*, 9 May 2007.

5 See also NSW Council of Civil Liberties, 'Australian phones 26 times more likely to be bugged than an American phone', *Media Release,* 13 January 2006.

6 Bronitt, S. and Stellios, J., 'Telecommunications interception in Australia: Recent trends and regulatory prospects', *Telecommunications Policy* 29 (2005), p. 886.

7 Bronitt, S. and Stellios, J., 'Telecommunications interception in Australia: Recent trends and regulatory prospects', *Telecommunications Policy* 29 (2005), p. 886. See also Bronitt and Stellios, 'Regulating Telecommunications Interception and Access in the Twenty-First Century: technological Evolution of Legal Revolution?', *Prometheus*, vol. 24, no. 4, December 2006, pp 413-428.

8. Before the Blunn Review, there were four major reports dealing with telecommunications interception. They were:

- The 1994 review by Mr P. Barrett into the Long Term Cost Effectiveness of Telecommunications Interception;

2.9 The Blunn Review observed that under Part 13 of the Telecommunications Act 'call data' may be accessed for security and law enforcement purposes subject to authorisation.[9]

2.10 The Blunn Review stated that generally the prescribed process for an authorisation involves an authorised officer of a designated agency certifying that disclosure is 'reasonably necessary' for the specified purpose, but under that process access to 'content or substance' is not to be disclosed. The Blunn Review therefore concluded:

> 1.7.2. Other than to reinforce the requirement that access should only be provided on receipt of a conforming certificate I see no reason to change that regime and I recommend accordingly.[10]

2.11 The Bill therefore clarifies the exceptions to disclosure of data in Part 13 of the Telecommunications Act and transfers these exceptions to proposed sections 175 and 176 (disclosure to ASIO) and proposed sections 178 to 180 (disclosure to enforcement agencies) of the TIA Act. In addition, the Bill sets up a new distinction between historical data and prospective data.

2.12 The Blunn Review did however raise issues with the current voluntary disclosure provisions in Part 13 which have led to some of the amendments contained in the Bill:

> 1.7.3. However in what seems to me to be anomalous provisions, subsections 282(1) and (2) provide for the disclosure or use of information or a document, including content or substance, by an 'eligible person' (apparently to anyone) without any certificate, if the disclosure or use is reasonably necessary for the enforcement of the criminal law or laws imposing a pecuniary penalty or for the protection of the public revenue.
>
> 1.7.4. The provisions are intended to allow disclosure where an employee of a carrier in the course of employment comes across information which is clearly relevant to the enforcement of the criminal law but the information has not been requested by a law enforcement agency.
>
> 1.7.5. In as much as they require the eligible person to form an opinion that disclosure is 'reasonably necessary' for the enforcement of the criminal law or the protection of the public revenue they appear inappropriate and sit oddly with the requirement established by subsections 282(3), (4) and (5)

- The 1999 review by Mr D. Boucher of Interception Arrangements under section 332R of the Telecommunications Act 1997;
- The 1999 review by Mr P. Ford of Telecommunications Interception Policy; and
- The 2003 review by Mr T. Sherman AO of Named Person Warrants and other matters.

9 A S Blunn AO, *Report of the Review of the Regulation of Access to Communications*, August 2005, p. 34.

10 A S Blunn AO, *Report of the Review of the Regulation of Access to Communications*, August 2005, p. 34.

> for a certificate from the requesting agency in which case access to content or substance is precluded.
>
> 1.7.6. That said, there is obviously a case for enabling eligible persons who do come across information in the course their employment which they consider relevant to security or law enforcement to report that to an appropriate authority. From a privacy point of view the provisions as presently drafted are not adequate and I recommend that they be reviewed with a view to clarifying the objective and better identifying the process to be followed. If they are to be retained, given the significance of the provisions, consideration should be given to them being incorporated in as a separate section.[11]

2.13 The Bill therefore contains proposed sections 174 and 177 to clarify that voluntary disclosure to ASIO or an enforcement agency is permitted.

2.14 The Office of the Privacy Commissioner's (OPC) submission to the Blunn Review in 2005 referred to previous recommendations it had made in relation to legislative review. OPC recommended that the operation of the TIA Act should be subject to overall independent review, including key stakeholder and public consultation at least every five years.

2006 amendments

2.15 As outlined in Chapter 1, the first tranche of the Blunn Review amendments contained more controversial measures than those contained in this Bill (such as stored communication warrants and B Party intercepts) and have already become law. The *Telecommunications (Interception) Amendment Act 2006* received Royal Assent on 3 May 2006.

2.16 The Senate Legal and Constitutional Legislation Committee made 28 recommendations in its report on the Telecommunications (Interception) Amendment Bill 2006 tabled in March 2006.

2.17 Only some of those recommendations specifically relate to the present Bill. Recommendation 17 regarding the *Spam Act 2003* is addressed by Schedule 2, Part 1, Item 5.

2.18 Committee Recommendation 25 called for a five year review of the amendments made by the 2006 Bill:

> 4.111 The Committee recommends that the Bill should include a provision for the provisions to expire in five years, with a review at that time or earlier.
>
> 4.112 The Review should encompass the broader issues surrounding the suitability and effectiveness of AAT members in the warrant issuing

11 A S Blunn AO, *Report of the Review of the Regulation of Access to Communications*, August 2005, pp 34-35.

> 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.

2.19 Following the Senate committee report, the government tabled several amendments to the Bill which were passed by Parliament. The Attorney-General stated in the House on 30 March 2006 that:

> ...this bill is to deal with matters that would otherwise be the subject of a sunset clause dealing with stored communications. We did not want to see those important measures come to an end, and that is why the legislation has been progressed not in haste but to ensure that these issues have been dealt with before that sunset clause comes into effect. The government will continue to consider in detail the committee report and the recommendations as part of its ongoing commitment to ensuring the regime achieves an appropriate balance. If there are further amendments that are thought to be appropriate following the consideration of the committee report, we will propose further amendments in the spring session of parliament.[12]

2.20 The government response to the Legal and Constitutional Legislation Committee report on the provisions of the Telecommunications (Interception) Amendment Bill 2006 was tabled in the Senate on 10 May 2007. Of the 25 recommendations made by the committee, the government accepted 18 in whole or in part. Recommendation 25 relating to a review was not accepted.

2.21 The Bill is not a response to the issues raised by the committee's 2006 report, but a separate legislative exercise.[13]

Summary of provisions

Commencement

2.22 Items 23 and 25 of Schedule 2 would apply the amendments made by Item 7 and Items 20 and 21 of that Schedule respectively, to conduct engaged in, or proceedings instituted, before or after the commencement of the respective items. The Scrutiny of Bills Committee has asked the Attorney-General for clarification of whether the operation of these provisions may affect any individuals' rights.[14] The Scrutiny of Bills Committee has not yet reported on the Attorney-General's response on this matter.

---

12 The Hon. Mr Philip Ruddock MP, Attorney-General, *House of Representatives Hansard*, 30 March 2006, p. 98.

13 This is confirmed by the Department in their *Answers to questions on notice*, 24 July, 2007p. 4. The Department provided, as Attachment A, an excel spreadsheet outlining the government's implementation of the Blunn Review thus far.

14 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No.7 of 2007*, p. 20.

Definitions

2.23 Schedule 1, Items 1 to 9 and Schedule 2, Items 2 to 12 amend definitions in section 5 of the TIA Act.

Telecommunications data

2.24 The Bill does not set out a definition of 'telecommunications data'.[15] Instead proposed section 172 provides that the provisions in proposed Chapter 4 of the Bill[16] do not permit the disclosure of the 'contents or substance of a communication.' Subject to this limitation, the provisions in Chapter 4 then authorise access to 'information or a document'.[17] The Explanatory Memorandum (EM) explains what material Chapter 4 is intended to authorise access to:

> Telecommunications data is information about a telecommunication, but does not include the content or substance of the communication. Telecommunications data is available in relation to all forms of communications, including both fixed and mobile telephony services and for internet based applications including internet browsing and voice over internet telephony.
>
> For telephone-based communications, telecommunications data includes subscriber information, the telephone numbers of the parties involved, the time of the call and its duration. In relation to internet based applications, telecommunications data includes the Internet Protocol (IP) address used for the session, the websites visited, and the start and finish time of each session.
>
> Telecommunications data specifically excludes the content or substance of a communication.[18]

2.25 The EM then elaborates further:

> Communications associated data will vary according to the type of telecommunications service. For fixed and mobile voice telephony, including voice calls, and voice- or text-messaging services, the term includes the details of the parties to the communication, the date, time and duration of the communication, the device used to send or receive the information, and (in some cases) the locations of the parties.
>
> For Internet based telecommunications, such as email, web browsing, instant messaging, or internet voice calls (Voice over Internet Protocol or VoIP), data includes the sender's and recipient/s' Internet addresses, the devices from which they were sent from or to, and the time and date at

---

15 The UK uses the term 'call associated data': see paragraph 21(4)(b) of the *Regulation of Investigatory Powers Act 2000* (UK).

16 See further discussion at paragraph 2.32.

17 This is comparable to the traditional use of Call Charge Records by law enforcement agencies.

18 p. 6.

which it was sent. The information does not include content such as the subject line of an email, the message sent by email or instant message or the details of Internet sessions.[19]

Enforcement Agency

2.26 The general definition of 'enforcement agency' is amended by Schedule 1, Item 6 by adding new paragraphs k and n:

(a) the Australian Federal Police; or
(b) a police force or service of a State; or
(c) the Australian Commission for Law Enforcement Integrity; or
(d) the ACC; or
(e) the Crime Commission; or
(f) the Independent Commission Against Corruption; or
(g) the Police Integrity Commission; or
(h) the Office of Police Integrity; or
(i) the Crime and Misconduct Commission; or
(j) the Corruption and Crime Commission; or
(k) an authority established by or under a law of the Commonwealth, a State or a Territory that is prescribed by the regulations for the purposes of this paragraph; or
(l) a body or organisation responsible to the Ministerial Council for Police and Emergency Management - Police; or
(m) the CrimTrac Agency; or
(n) any body whose functions include:
(i) administering a law imposing a pecuniary penalty; or
(ii) administering a law relating to the protection of the public revenue (emphasis added).

2.27 The EM states:

Item 6 amends subsection 5(1) to include a definition of 'enforcement agency'. An authorised officer of one of these bodies will be able to authorise the disclosure of historical telecommunications data. The definition draws together the agencies described as 'criminal law-enforcement agency', 'civil penalty-enforcement agency' and 'public revenue agency' in section 282(10) of the Telecommunications Act. The definition includes bodies covered by the definition of 'criminal law-enforcement agency' in this subsection, as well as a body or organisation responsible to the Ministerial Council for Police and Emergency Management – Police, the CrimTrac Agency or any other body whose functions include administering a law imposing a pecuniary penalty or a law relating to the protection of the public revenue.[20]

19 p. 8.

20 p. 4.

Authorised officer

2.28 Item 2 also amends the definition of an 'authorised officer' of an enforcement agency. The EM states:

> The formulation of the definition reflects the differing management structures of enforcement agencies, particularly in the case of criminal law-enforcement agencies. An authorised officer has the power to authorise the disclosure of telecommunications data.[21]

2.29 Schedule 1, Item 10 inserts new section 5AB to give the head of an enforcement agency the authority to authorise a particular management position or management office in their organisation for the purposes of paragraph (c) of the definition of authorised officer in subsection 5(1). The EM states that this will 'allow persons holding the authorised position or office to authorise the lawful disclosure of historical telecommunications data, or in the case of criminal law-enforcement agencies, historical and prospective telecommunications data'.[22]

Security authority

2.30 Schedule 2, Items 3 and 4 amend subsections 5(1) and 5(4A) to include a new definition of 'security authority' and to clarify who is defined as an employee of a security authority. Proposed subsection 5(4A) will provide that an employee of a security authority includes a person 'whose services are made available to the security authority'.

Transfer of provisions

2.31 The remainder of Schedule 1 generally transfers key security and law enforcement provisions from Parts 13, 14 and 15 of the Telecommunications Act to the TIA Act.[23]

2.32 Schedule 1, Item 12 inserts new Chapter 4 dealing with access to telecommunications data. The amendments establish a regime for particular officers of ASIO or an enforcement agency to lawfully authorise the disclosure of telecommunications data without breaching the general prohibitions on the disclosure of telecommunications data in existing sections 276, 277 and 278 of the Telecommunications Act.

2.33 The amendments create a new two tier access regime. The first tier encompasses the traditional access to existing telecommunications data (proposed

---

21 p. 3.

22 p. 5.

23 The Department has set out the transfer of provisions in table form: see Additional Information No. 2, Diagrams tabled by Attorney-General's Department, Telecommunications and Surveillance Law Branch at the public hearing held in Canberra on Monday 16 July 2007, available from the committee's website.

sections 175, 178 and 179). The second tier which would be limited to a narrower range of agencies and would require a higher threshold of authorisation, allows for access to future telecommunications data (proposed sections 176 and 180).

2.34 The justification for the new two tier access regime for data is stated in the EM:

> The need to distinguish between historical and prospective data is a reflection of the advances in technology which enables the use of telecommunications data to provide location information. To reflect the increased privacy implications of access to prospective telecommunications data, three more restrictive conditions are attached to these authorisations:
>
> - restricting the disclosure of prospective telecommunications data to an authorised officer of a criminal law-enforcement agency, for the investigation of offences which attract a maximum term of imprisonment of at least 3 years;
> - limiting the timeframe for which an authorisation may be in force to 45 days; and
> - requiring the authorising officer to have regard to the impact of the authorisation on the privacy of the individual concerned.[24]

2.35 Proposed sections 174 and 177 deal with voluntary disclosures of telecommunications data by employees of carriers or carriage service providers to ASIO and enforcement agencies. These provisions make it clear that they only apply in the case of voluntary disclosures and that requests from agencies must be dealt with under proposed sections 175, 176 and 178-180.

2.36 There are certain safeguards set out in the Bill in relation to access to telecommunications data. Authorisations must be retained for a period of three years (proposed section 185). The head of an enforcement agency must report on the number of authorisations to the Minister on an annual basis, and this report must be tabled in Parliament (proposed section 186).

2.37 Schedule 1, Item 41 amends the Telecommunications Act by inserting proposed section 306A. This provision is based on the existing record keeping arrangements for the disclosure of historical communications associated data under section 306 of the Telecommunications Act. Proposed section 306A provides for the records of prospective authorisations made under the TIA Act that are to be kept by carriers, carriage service providers and number-database operators.

2.38 Finally, proposed section 182 creates offences for unlawful disclosure or use, including secondary use and disclosure, of telecommunications data.

---

24 p. 12.

Carrier cooperation with interception agencies

2.39 Schedule 1, Item 12 inserts new Chapter 5 dealing with cooperation with interception agencies. New Part 5.3 requires carriers and carriage service providers to ensure that communications carried over their telecommunications system are capable of being intercepted ('interception capability' is defined in proposed subsection 187(2)). New Part 5.5 deals with the obligation on carriers that the intercepted information is capable of being delivered to interception agencies from a delivery point ('delivery capability' is defined in proposed subsection 187(3)). Proposed section 188 provides a process for defining 'delivery points', including the resolution of any disagreements by the Australian Communications and Media Authority (ACMA).[25]

2.40 The Attorney-General may make written determinations on the interception capability of certain carriage services under proposed section 189. The new post of the Communications Access Coordinator (CAC) is defined by proposed section 6R (previously 'agency coordinator') and may grant exemptions to any interception capability obligations under proposed section 192. ACMA can also grant exemptions for trial services under proposed section 193.

2.41 Carriers also have to prepare and submit an annual 'Interception Capability Plan' (ICP) in accordance with new Part 5.4. The plans are now lodged with the CAC rather than ACMA.

2.42 New Part 5.6 preserves existing cost allocation principles between the telecommunications industry and interception agencies associated with interception and delivery capability.[26]

Exemptions

2.43 Proposed subsections 192(4), 195(6) and 203(4) to be inserted by Item 12 of Schedule 1, state that various instruments are not legislative instruments. The Scrutiny of Bills Committee noted that, in each case, the EM (at pages 20, 22 and 27 respectively) states that the reason these exemptions are not legislative instruments is that the relevant documents contain sensitive and confidential information. For example, in respect of the instrument referred to in proposed subsection 192(4), the EM explains that if the 'documents were not kept confidential, the limitations of interception capability and, by implication, how to avoid interception, could become

---

25 The Department has set out interaction with CSPs diagrammatically: see Additional Information No. 2, Diagrams tabled by Attorney-General's Department, Telecommunications and Surveillance Law Branch at the public hearing held in Canberra on Monday 16 July 2007, available from the committee's website.

26 Members of the Australian Mobile Telecommunications Association (AMTA) do not charge police for services in life-threatening situations but are entitled, under the Telecommunications Act, to recover costs for non-life threatening requests from police for call records to assist criminal investigations.

publicly apparent.' However, the Scrutiny of Bills Committee pointed out inconsistencies in the EM which refers to exemptions granted by ACMA under proposed subsection 193(1) as administrative in nature. That committee queried why:

> …despite appearing to be very similar provisions, the exemption provided for under proposed new subsection 192(1) is considered to be legislative in character but the exemption provided for in proposed new subsection 193(1) is considered administrative in nature.[27]

2.44 The Scrutiny of Bills Committee has sought the Attorney-General's advice as to whether, if the exemption under proposed subsection 193(1) is administrative in nature as suggested by the EM, it should be subject to merits review under the *Administrative Appeals Tribunal Act 1975*.

Schedule 2 amendments

Child pornography

2.45 Schedule 2, Items 6 and 7 amend section 5D of the TIA Act to ensure that the list of 'serious offences', for which interception warrants may be sought, includes all child pornography offences, whether or not the penalty for such an offence is imprisonment for at least 7 years. Child pornography offences are already defined as 'serious offences' by subparagraphs 5D(2)(b)(viii) and (ix) but only where the maximum penalty is imprisonment for at least seven years.

Spam Act

2.46 The TIA Act provides that interception material can be adduced as evidence in an exempt proceeding. Schedule 2, Item 5 widens the definition of 'exempt proceedings' to allow disclosures for the purposes of proceedings in relation to the *Spam Act 2003*.[28] This amendment is consistent with the intention of recommendation 17 of the Senate Legal and Constitutional Legislation Committee's report on the Telecommunications (Interception) Amendment Bill 2006.[29]

Testing interception capabilities

2.47 The Bill contains several amendments to partially implement recommendation 24 of the Blunn Review, which recommended allowing access to the content of communications for the protection of data systems and the development or testing of new technologies.[30] Schedule 2, Item 16 inserts new Part 2.4 in the TIA Act which

---

27 Senate Standing Committee for the Scrutiny of Bills, *Alert Digest No.7 of 2007*, p. 19.

28 EM, p. 41.

29 pp 25-26.

30 The Department has provided a table of the policy origin of the amendments in Schedule 2 as Attachment B to *Answers to questions on notice taken at the hearing*, 24 July 2007.

will allow the Attorney-General to authorise interception for developing and testing interception capabilities, subject to conditions, and only by security agencies.

2.48 Schedule 2, Items 11 and 12 would amend existing subsections 5F(2) and 5G(2). These provisions currently create a general exemption to the definition of 'passing over the telecommunications system' for the purpose of a computer network operated by or on behalf of the Australian Federal Police (AFP). People who operate, protect or maintain the network, or are responsible for the enforcement of professional standards in the AFP are treated as 'intended recipients' so that their monitoring of outbound and inbound communications is not unlawful. These provisions were inserted by the 2006 amendments and were subject to a two year sunset clause.

2.49 Items 11 and 12 would expand the exemption from the AFP to cover Commonwealth agencies (the AFP, the Australian Commission for Law Enforcement Integrity and the Australian Crime Commission), security authorities (ASIO, the Department of Defence, and the Department of Foreign Affairs and Trade) and eligible authorities of the States (integrity and crime commissions and police forces). The EM states that:

> Item 11 widens the existing provisions to increase the number of agencies who may monitor all outbound and inbound communications for the purposes of enforcing professional standards and protecting and maintaining their corporate network. This is achieved by ensuring that monitoring, recording or copying a written communication while it is still in the 'confines' of the network is not interception for the purposes of the TIA Act.[31]

31 p. 42.

CHAPTER 3

KEY ISSUES

3.1 This chapter examines the main issues and concerns raised in the course of the committee's inquiry. Submissions to the inquiry were generally favourable to the Bill, especially the desirability of a single comprehensive legislative regime dealing with access to telecommunications information.[1]

3.2 Two submissions, from Electronic Frontiers Australia (EFA) and the Australian Privacy Foundation (APF), suggested that the Bill is so flawed that it should not be passed. These organisations focused on privacy implications of the new regime for access to telecommunications data. Several organisations recommended the Bill be passed with minor amendments, many of which involve limiting the language of various definitions in the Bill.

3.3 The main issues raised include:

- the definition of key terms such as 'enforcement agency' in the Bill;
- the lack of a definition of 'telecommunications data';
- privacy concerns, particularly in relation to access to prospective telecommunications data and the impact of the secondary disclosure provisions on police officers;
- the obligations on telecommunications companies;
- concerns about whether the amendments meet the need to protect critical infrastructure; and
- the mechanisms for reporting, oversight and review.

Consultation

3.4 The amendments in the Bill were the subject of a consultation process run by the Attorney-General's Department.[2] An officer of the Department outlined the consultation undertaken:

> [W]e developed the draft legislation in close consultation with Commonwealth government agencies. That was an internal consultation process. We released the exposure draft of the bill in February [2007] and we received 32 submissions addressing the various provisions. To follow up on that we also had a number of meetings and conversations with

1 See, for example, Optus, *Submission 2;* Department of Defence, *Submission 3*; Communications Alliance Ltd, *Submission 18*, p. 1; Tasmania Police, *Submission 23*, p. 2.

2 Full details about the consultation process are given by the Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, pp 4-8.

> industry groups and various submitters to work through some of the issues that they raised. Quite a few of the issues that they have raised have resulted in amendments between the exposure draft and the [bill] that was subsequently introduced.[3]

3.5 The Office of the Privacy Commissioner (OPC) noted that 'a number of the issues raised in our previous submission have been addressed in the Bill and Explanatory Memorandum'.[4] Similarly, Mr Chris Althaus of the Australian Mobile Telecommunications Association (AMTA) commented at the hearing that:

> There was over an extended period a high degree of interaction with the industry. We had a number of concerns particularly in relation to standards and powers within the exposure draft. We were able to put an argument forward, the government listened to that, and that was an important amendment in our view. In many respects it was the most important amendment that came forward.[5]

Definitions

Definition of 'enforcement agency'

3.6 EFA submitted that CrimTrac should be deleted from the definition of 'enforcement agency' on the basis that it is not a criminal law enforcement agency or an agency that conducts investigations.[6] EFA was also concerned that the inclusion of CrimTrac in the definition of 'enforcement agency' would give CrimTrac access to stored communications warrants under section 110 of the TIA Act.[7]

3.7 The Law Council of Australia (Law Council) expressed concern at the inclusion of paragraph (k) in the proposed definitions of 'enforcement agency' and 'criminal law-enforcement agency'. This provision allows an authority established under a Commonwealth, state or territory law to be added to these definitions by regulation. The Law Council was particularly concerned that this would allow delegated legislation to expand the range of agencies which will be able to authorise access to prospective telecommunications data:

> The Law Council believes that the practice of reserving to the Executive the power to expand definitions of this nature, which are crucial to scope and operation of the TIA Act, is of great concern. No reason has been provided

---

3 *Committee Hansard*, 16 July 2007, p. 30.

4 *Submission 19*, p. 2.

5 *Committee Hansard*, 16 July 2007, p. 18. See also Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, pp 4-5.

6 *Committee Hansard*, 16 July 2007, p. 10. See also Law Council of Australia, *Submission 20*, p. 14.

7 *Submission 6a*, p. 5.

for why the efficient operation of the TIA Act requires the sort of flexibility afforded the Executive under paragraph (k).[8]

Departmental response

3.8 In relation to the inclusion of CrimTrac in the definition of 'enforcement agency', an officer of the Department advised:

> [CrimTrac] are an enforcement agency in terms of telecommunications data. That is an existing provision under the Telecommunications Act…At this stage we have transferred over the agencies provided within the definition of 'enforcement agency' under the Telecommunications Act and we are looking to see whether or not it is appropriate that they continue to be within that definition. Until such time as we can actually establish that it is not appropriate, we have not removed them.[9]

3.9 The Department explained further:

> The inclusion of CrimTrac in the definition of an enforcement agency in the TIA Act will not in itself allow CrimTrac to access stored communications. Stored communications may only be accessed by an enforcement agency where they have satisfied an issuing authority that the information that would be obtained would likely assist in connection with the requesting agencies investigation of a serious contravention, being an offence punishable by imprisonment for a maximum period of 3 years.
>
> As CrimTrac's functions do not include the investigation of any offences, they will not be eligible to be issued with a stored communications warrant.[10]

3.10 On the issue of the power to expand the definitions of 'enforcement agency' and 'criminal law-enforcement agency' by regulation, the Department responded:

> The regulation making provision is a direct transfer from the Telecommunications Act which provides for an agency to be prescribed as a 'criminal-law enforcement agency'. While there are no agencies currently proposed to be prescribed, the regulation making power will allow the inclusion of agencies where their investigative functions change to the extent that access to prospective information becomes necessary.
>
> For example, the Australian Customs Service and the Australian Securities and Investment Commission currently have access to historical data. If the nature of their investigative functions change to the extent that it is considered appropriate for them to receive telecommunications data in near-real time, they may be prescribed under paragraph 5(1)(k) of the TIA Act.[11]

---

8 *Submission 20,* p. 13.

9 *Committee Hansard,* 16 July 2007, p. 10.

10 *Answers to questions on notice*, 24 July 2007, p. 22.

11 *Answers to questions on notice*, 24 July 2007, p. 10.

Meaning of 'telecommunications data'

3.11 There is no definition of 'telecommunications data' in the Bill. Instead, proposed section 172 prevents the provisions which permit the disclosure of telecommunications data from applying to the 'contents or substance of a communication'. Subject to this limitation, the provisions in Chapter 4 then authorise access to 'information or a document'.

3.12 In its comments on the Exposure Draft of the Bill, OPC suggested that the distinctions between 'information or a document' and 'contents or substance' may be difficult to discern in some cases and called for further clarification, given that the prohibitions against disclosure in the TIA Act attract a serious penalty.[12] OPC welcomed the inclusion in the EM of material to clarify the distinction between call data and the content of a communication.[13]

3.13 However, the APF and EFA felt that these changes did not go far enough and expressed particular concern about the potential to access information about web browsing and chat room sessions, and email header data as telecommunications data.[14] APF argued:

> We are very disappointed that such a fundamental revision of the relevant provisions has missed the opportunity to more clearly define what is meant by key terms such as 'telecommunications data' and 'content or substance'. This creates unacceptable ambiguity and uncertainty about the 'reach' of the various powers and protections. It also leaves open the possibility that very sensitive information such as mobile phone location data, email message headers and various Internet logs would not be considered 'substance or content' or stored 'communications', and would therefore be subject not to the TIAA warrant controls but to the much weaker protection applying to 'authorisations'…We submit that a much clearer legislative distinction between 'traffic data' and 'substance and content' is required.[15]

3.14 Similarly, EFA suggested that the distinction between the content or substance of a message and other data was particularly unclear in relation to email header data:

> In our view the subject line is part of the content of a message, but existing legislation is silent on this matter and it cannot be known whether the same view would be held by all carriers and enforcement agencies. Furthermore, email messages can carry significantly more…information in the header section than is equivalent to 'traffic information' associated with telephone

---

12 Office of the Privacy Commissioner, *Submission on Exposure Draft of the Telecommunications (Interception and Access) Amendment Bill 2007*, February 2007, at http://www.privacy.gov.au/publications/subtel0207.html (accessed 1 July 2007).

13 *Submission 19*, p. 2.

14 *Submission 6*, pp 9-12; *Submission 17*, p. 3.

15 *Submission 17*, p. 3.

> calls. For example, some (probably most) email programs enable the end-user to create their own special header fields in outgoing messages, in which they can place any information they wish.[16]

3.15 As a result, EFA suggested that clarification of the distinction between data and content in relation to email messages should be included in the Bill.[17]

3.16 EFA further argued that the Bill should be amended so that access to information regarding Internet sessions would only be permitted under a stored communications warrant.[18] EFA submitted that the data which may be captured in relation to Internet sessions is qualitatively different to telecommunications data about telephone calls and email messages:

> Surveillance of web browsing activities is akin to filming individuals' activities in a manner that records every item they purchase in shops, every film they see at the cinema or hire or buy, every book and magazine they glance through and/or purchase or take out on loan from a library and so on. Furthermore, unlike 'telecommunications data' about telephone calls and email messages, the address of a web page often, of itself, provides information about the content or substance of the communication and web page addresses can be used to obtain access to the content that was communicated.[19]

Departmental response

3.17 The Department advised that there was no intention to insert a definition of 'telecommunications data' into the Bill and explained:

> Our concern about defining what technology and call associated data may be now [is that the definition] might be redundant in 12 months time. Essentially we rely on the premise that the contents and substance of a communication are protected and are only accessible under a TIA warrant, an interception warrant or a stored communication warrant, and it is the other information that attaches to a communication but does not disclose the contents or the substance of that communication that is the associated data. One of the points of bringing this all into one piece of legislation is the hope that by having the three limbs together it will be clearer when advising law enforcement and the carriers on what exactly is content and what is call associated data as new technologies come into place.[20]

---

16 *Submission 6*, p. 9.

17 *Submission 6*, pp 9-10. The Department has agreed to review the EM to remove any ambiguity. See Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, p. 13.

18 *Submission 6*, p. 12.

19 *Submission 6*, p. 4.

20 *Committee Hansard*, 16 July 2007, p. 22.

3.18 The EM states that the subject line of an email or details of Internet sessions are not captured as 'telecommunications data'.[21] At the hearing, an officer of the Department clarified what information would be captured as telecommunications data in relation to web browsing:

> In relation to getting call-associated data regarding an IP [Internet Protocol] address that can identify a web page, that is not content because all it does is tell a law enforcement agency that a certain target went to a certain website. It does not tell them any other details. It does not tell them that they then went into their bookings online or via their travel agent or that they downloaded particular information. It does not give them any knowledge of the substance as to why they were on that web page. URLs [Uniform Resource Locators] are a little different because they will then point out the continuum of where the person actually went to.[22]

3.19 The Department went on to argue that URL data was equivalent to a telephone number in terms of the information provided:

> With regard to web URLs—or URIs [Uniform Resource Identifiers] —and how an apparatus finds that on the Internet, I will go back to the analogy of when we used to make telephone calls; if we had call charge records we would have a list of numbers that a person called but it does not show content...If an officer wants to phone those numbers and find out what they are they could ring them systematically. It is the same with a computer. When they go and click that button to search that URL, it is the same thing.[23]

3.20 The Department also responded to EFA's concerns that email header data may be captured as telecommunications data:

> EFA in their submission provided an example that relates to user-defined 'headers' to email messages. EFA states that whilst headers generally do not contain personal information or content, there is the capacity to include information in headers which are defined by the user. They argue that there is therefore confusion as to whether this information is considered data or content.
>
> The EFA rely on an Internet Engineering Task Force (IETF) standard referred to as Request for Comment (RFC) 822. This is an obsolete standard that was superseded in 2001 by RFC 2822 and the relevant header fields stated by EFA cannot be found in the current standard. RFC 2822 also states that these obsolete fields 'MUST NOT be generated'.[24]

---

21 p. 8.

22 *Committee Hansard*, 16 July 2007, p. 31.

23 *Committee Hansard*, 16 July 2007, p. 31.

24 Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, pp 10-11. The EFA disputes the Department's interpretation of RFC 2822: see *Submission 6b*.

Privacy concerns

3.21 Several submissions raised concerns regarding the impact the Bill would have on privacy, in particular the provisions relating to access to prospective telecommunications data and to secondary disclosure of data.

Access to prospective telecommunications data

3.22 EFA expressed concerns about the potential use of real time access to telecommunications data to track individuals using data obtained from mobile telephones. EFA stated, in relation to prospective data, that:

> New technologies such as Assisted GPS, reportedly expected to be introduced in Australia by some carriers in 2007 or 2008, will greatly improve the accuracy of mobile phone location information. Access to 'prospective' location information enables not only identifying/tracking location but potentially real world, real time, surveillance of a tracked individual's activities.[25]

3.23 EFA therefore submitted that access to prospective mobile telephone data should be subject to more stringent control than authorisation by certain officers in ASIO or a criminal-law enforcement agency:

> [W]e are very concerned that this bill will enable tracking of people via mobile phone location information without a warrant, which is basically further extending the definition of 'telecommunications data'…This bill appears to have the specific purpose of allowing law enforcement agencies to use a person's own tracking device that they carry with them all of the time. Because it is a device that can be used to track a person without the need to covertly install a tracking device on a person's property or body, we believe that there is considerably more potential for misuse of these new powers. We are strongly of the view that for that kind of information to be collected in near real time, because it will enable physical visual of track people, a warrant should be required similar to the existing surveillance device warrants in the Commonwealth and the various states, or with similar conditions attached as the stored communications warrants.[26]

3.24 The Law Council acknowledged that the Bill places greater controls on access to prospective telecommunications data (under proposed sections 176 and 180) than access to existing data (under proposed sections 175, 178 and 179). However, the Law Council considered that these controls do not go far enough.[27] The Law Council also argued that criminal law-enforcement agencies should require a

---

25 *Submission 6*, p. 4.

26 *Committee Hansard*, 16 July 2007, p. 9. See also New South Wales Council for Civil Liberties, *Submission 10*, p. 3; Australian Privacy Foundation, *Submission 17*, p. 4.

27 *Submission 20*, p. 6.

warrant in order to access prospective telecommunications data and thus use a person's mobile telephone as a tracking device:

> The Law Council recognises that under Section 39 of the Surveillance Devices Act 2004, law enforcement officers are already able to use a tracking device without a warrant in the investigation of a federal offence which carries a maximum penalty of at least 3 years. This is provided that written permission is received from an 'appropriate authorising officer' and installation and retrieval of the device does not require entry onto premises without permission or interference with the interior of a vehicle without permission.
>
> Nonetheless, the Law Council believes that the ease with which telecommunications data may be used to track a person, as compared to the difficult of secretly affixing a physical tracking device to a person or thing, renders proposed s 180 far more amenable to misuse or overuse by law enforcement agencies than existing provisions in the Surveillance Devices Act 2004.
>
> It is on that basis that the Law Council believes that access to prospective telecommunications data should require a warrant.[28]

3.25 The Queensland Council for Civil Liberties also expressed concern that the Bill would allow mobile telephone location information to be disclosed under a written authorisation for a period of 45 or 90 days without the need to obtain a warrant.[29]

Departmental response

3.26 The Department noted that the Telecommunications Act already provides for enforcement agencies to access prospective telecommunications data:

> Access to prospective data already exists under the current regime. In moving it over to the TIA act, we have acknowledged that there are two accesses under section 282 of the act—that is, historical data and information in real time.[30]

3.27 In response to concerns about the privacy implications of access to prospective data from mobile telephones, the Department argued that the new regime imposes more stringent requirements for access to prospective data:

> From our perspective that is addressed by the fact that we have acknowledged that there is potentially a greater breach of privacy if a person can access prospective data, and that is why we have separated it out from historical data. We have placed a time limitation on it. We have also limited the agencies that can access this information to criminal law

28 *Submission 20*, pp 6-7.

29 *Submission 8*, p. 2.

30 *Committee Hansard*, 16 July 2007, p. 23.

> enforcement and national security agencies, and we have made it an offence that is punishable by three years, which is consistent with the surveillance devices legislation.[31]

Secondary disclosure provisions

3.28 The Police Federation of Australia (Police Federation) held concerns regarding how proposed section 182 may impact on the privacy rights of police officers, especially those involved in disciplinary proceedings.[32] Proposed section 182 would allow the secondary disclosure and use of telecommunications data where the disclosure is reasonably necessary 'for the enforcement of a law imposing a pecuniary penalty'. At the hearing, Mr Mark Burgess of the Police Federation explained that:

> the disciplinary offences applicable to most police jurisdictions are found within state and territory legislation and have provisions for pecuniary penalties by way of fines even for very minor matters.[33]

3.29 Mr Burgess gave further evidence that:

> We are concerned that the bill will give the ability to disclose information, as limited as it might be, which will therefore allow people to undertake fishing expeditions for further information that they might think they can gather, and when they might not have been aware of any of this in the first place. This is not about preventing appropriate use of this legislation or this bill to target police officers undertaking criminal or corrupt activities. Our concern centres around the prospect of it being used in respect of what all of us in this room would consider to be minor disciplinary issues. Because the relevant legislation that underpins those disciplinary issues has provisions for monetary penalties, they will be picked up.[34]

3.30 The Police Federation argued that the definition of 'pecuniary penalty' in the Bill should be narrowed or the reference deleted. In the alternative, the Police Federation submitted that the secondary disclosure provision should exempt police disciplinary proceedings.[35]

3.31 On the other hand, the NSW Ombudsman argued that the current restrictions on secondary disclosure are too narrow and that secondary disclosure of telecommunications data to the Ombudsman to support its role in investigating police misconduct should be permitted.[36] The Western Australian Police also supported

---

31 *Committee Hansard*, 16 July 2007, p. 24.

32 *Submission 4*, pp 1-3.

33 *Committee Hansard*, 16 July 2007, p. 2.

34 *Committee Hansard*, 16 July 2007, p. 3.

35 *Submission 4*, pp 2-3.

36 *Submission 7*, pp 1-2.

allowing secondary disclosure of telecommunications data, such as call charge records, for the purpose of police disciplinary proceedings.[37]

Government response

3.32 The Police Federation submitted correspondence from the Attorney-General which explained that the bill 'permits the secondary disclosure of information to an agency in circumstances where the receiving agency would itself have been able to access the information directly from the carrier.'[38] The Attorney-General also noted that the meaning of 'pecuniary penalty' is 'limited to specific monetary penalties set out in relevant legislation and imposed by a court. The term does not include administrative sanctions that may have a financial impact, such as for example, a demotion'.[39]

3.33 The Department gave further evidence regarding the difficulties involved in excluding police disciplinary proceedings which impose a pecuniary penalty from the operation of proposed section 182:

> In general terms it would not be appropriate to exclude pecuniary penalties overall. Obviously under some of the individual state and territory police acts some of the pecuniary penalties that would trigger the secondary disclosure provisions would be quite serious. Given that 'pecuniary penalty' is a fairly broad term, the alternative would be to try to insert more detailed definitions that relate and encompass all those different state and territory police acts. Before we did that we would need to consult closely with each of the state and territory police commissioners. It should also be said that, because the definitions in question that are giving the Police Federation trouble are in the state and territory legislation, our view is that it is probably better that they deal with it as a matter under the state employment legislation.[40]

Consideration of privacy implications

3.34 Privacy NSW commented favourably on the requirement in proposed subsection 180(5) for an authorised officer to have regard to likely interference with the privacy of individuals when giving authorisation for access to prospective telecommunications data.[41] Privacy NSW suggested proscribing (by way of regulation or similar) a requirement to have each enforcement agency (to whom

37 *Submission 21*, p. 2.

38 *Submission 4*, attachment, p. 2.

39 *Submission 4*, attachment, p. 2.

40 *Committee Hansard*, 16 July 2007, pp 30-31. See further Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, pp 11-12.

41 *Submission 16*, p. 1.

authorising officers belong) develop guidelines on how the privacy implications of an authorisation should be considered and documented.[42]

3.35 OPC made a similar recommendation that authorised officers be provided with practical guidance, in the form of a note to the Bill or detail in the EM, to assist them in discharging the obligation in proposed subsection 180(5).[43]

3.36 Privacy NSW and OPC also made recommendations regarding proposed paragraph 189(4)(c) which provides that the Minister, before making determinations in relation to interception capabilities, must take into account the privacy of the users of telecommunications systems.[44] In particular, OPC suggested:

> …the inclusion of a note to the clause, or in the explanatory memorandum, which provides guidance about how the privacy of telecommunications users will be taken into account in the making of the determination.[45]

3.37 In the same vein, NSW Council for Civil Liberties welcomed the inclusion of privacy as a consideration in proposed sections 180, 183 and 189 but suggested that there should be 'further elaboration of this requirement in the Bill by way of substantive requirements for protection of privacy.'[46]

Departmental response

3.38 The Department noted that the issue of providing further guidance on the consideration of interference with privacy under proposed subsection 180(5) had been raised during consultation on the Exposure Draft and advised that:

> The Government did not agree with the recommendation to include further legislative guidance on consideration of privacy. Consideration of privacy issues will vary enormously according to the unique circumstances of each situation. In particular, this may include the relationship between the seriousness of the offences being investigated, the value of information likely to be obtained, and the extent to which accessing this information would, in the circumstances, breach an individual's privacy.
>
> However, these are matters that the CAC [Communications Access Coordinator] may wish to address in the procedural requirements provided for in new section 183.[47]

---

42 *Submission 16*, p. 1.

43 *Submission 19*, p. 2.

44 *Submission 16*, p. 1; *Submission 19*, p. 4.

45 *Submission 19*, p. 4.

46 *Submission 10*, p. 2.

47 *Answers to questions on notice*, 24 July 2007, p. 5.

Destruction of data

3.39 Proposed sections 174 and 177 deal with voluntary disclosures of telecommunications data to ASIO and enforcement agencies by employees of a carrier or carriage service provider. OPC suggested that these provisions include:

> …positive obligations on law enforcement agencies to destroy irrelevant material containing personal information collected under these provisions together with information which is no longer needed by such law enforcement agencies and to do so in a timely manner.[48]

Departmental response

3.40 The Department advised in relation to this suggestion that:

> The Government will consider this recommendation, but notes reservations about the need for such an amendment. [49]

3.41 In particular, the Department suggested an amendment may not be required due to the limitation that proposed section 181 would place on the *use* of data lawfully disclosed under the TIA Act:

> [T]he limitation on the use of information under section 181 means that information can only be used in relation to a lawful disclosure of telecommunications data, and that the use is in connection with that lawful disclosure. This means that telecommunications data which is irrelevant to a criminal investigation cannot be lawfully used. It is our view that this provision provides an equal protection as the need to destroy irrelevant information.[50]

Obligations on carriers and carriage service providers

3.42 While submissions from the telecommunications industry generally supported the Bill, they suggested minor amendments to the provisions relating to obligations on telecommunications companies.

Communications Access Coordinator

3.43 AMTA suggested amendments to proposed section 6R to require the CAC to act in accordance with the objects and regulatory policy of the Telecommunications Act in the performance of his or her duties under Chapter 5 of the TIA Act.[51] Mr Chris Althaus of AMTA noted:

---

48 *Submission 19*, p. 3.

49 *Answers to questions on notice*, 24 July 2007, p. 16.

50 *Answers to questions on notice*, 24 July 2007, p. 19.

51 *Submission 5*, p. 2.

> The Communications Access Coordinator role seems to be one that is particularly pivotal and we would like to see the objectives of the Telecommunications Act picked up by the CAC…[52]

3.44 Vodaphone also considered that the replacement of the existing provisions regarding 'agency coordinator' in the Telecommunications Act with the new provisions establishing the CAC in the TIA Act resulted in:

> …a lack of guidance afforded to the role of Communications Access Co-ordinator in the conduct of its functions where previously there existed at least some degree of clarity. This arises as a result of the removal of provisions under the *Telecommunications Act 1997* that mandated that certain objects of the legislation were to be borne into account in the exercise of these Co-ordinator's functions.[53]

Departmental response

3.45 An officer of the Department gave evidence that the amendment proposed by AMTA to the definition of the CAC was unnecessary:

> The objects of the Telecommunications Act are picked up under several of the powers of the Communications Access Coordinator…The role of the CAC is to make decisions on behalf of law enforcement—national security—in relation to particular things, so we are not sure that it would add anything. The definition, except for the change of the name from the agency coordinator, is exactly as it has been since 1997 and it has worked extremely successfully.[54]

Delivery points

3.46 AMTA and Telstra expressed concerns regarding the factors ACMA will take into account when determining delivery points under proposed subsection 188(6).[55] AMTA explained that:

> …meeting the Delivery Capability requirements often involves the installation of specialised equipment for this purpose. In practical terms, the location of a delivery point will be affected by the physical location of equipment performing the Delivery Capability function. Therefore, the factors to be considered in determining Delivery Points should also take account of the location of any equipment performing Delivery Capability functions.[56]

---

52 *Committee Hansard*, 16 July 2007, p. 13.

53 *Submission 11*, p. 2.

54 *Committee Hansard*, 16 July 2007, p. 28.

55 *Submission 5*, p. 6; *Submission 9*, p. 1.

56 *Submission 5*, p. 6.

Departmental response

3.47 In evidence to the committee, the Department noted that proposed section 188 did not alter the existing arrangements under the Telecommunications Act in relation to delivery points. The Department also explained that, under proposed section 188, carriers will nominate delivery points in the first instance.[57] It is only where a carrier and an interception agency cannot agree on a delivery point that ACMA will be required to make a determination under proposed subsection 180(5).

Interception capabilities

3.48 AMTA and Telstra objected to the definition of 'interception capability' in proposed subsection 187(2).[58] In particular, AMTA was concerned that:

> …the proposed definition includes any equipment connected to a telecommunications network. Provision of services in an Internet environment involves use of a variety of separate components that are clearly defined in the *Telecommunications Act 1997*, including customer equipment, carriage services, that is, the carrying of Internet 'packets' across networks and Internet applications and content services, such as instant messaging and web hosting. For the most part Internet applications, content services and customer equipment can be independent of the Carrier or CSP [Carriage Service Provider].[59]

3.49 AMTA suggested changes to the definition in proposed subsection 187(2) to provide that interception capability is not required in relation to 'customer equipment', or equipment supplying a 'content service', as these terms are defined in the Telecommunications Act.[60]

3.50 Vodaphone also submitted that:

> Some clarification may be required in the area of converged services with the apparent grouping and classification of Internet content services and applications onto the existing responsibilities of Carriers and Carriage Service Providers. These obligations appear to be imposed without adequate consideration given to the nature of proprietary applications and attention to the inability of Carriers to apply operational control over such matters as third party equipment.[61]

---

57 *Committee Hansard*, 16 July 2007, p. 27.

58 *Submission 5*, pp 2-3; *Submission 9*, p. 4.

59 *Submission 5*, pp 2-3.

60 *Submission 5*, p. 3.

61 *Submission 11*, p. 2.

Departmental response

3.51 The Department explained that where equipment is not within the control of carriers they will not have an obligation to provide interception capability. However, an officer of the Department noted:

> AMTA were talking about customer premise equipment and they referred to the Telecommunications Act. Within the Telecommunications Act 'customer premise equipment' refers to the equipment that resides within the premise of the customer—for example, mainframes, network terminating units, routers and switches. They gave examples of how in the new technology age these are becoming less in control of the carrier. In our view in some cases in the industry they manage or remotely manage those routers, switches or mainframes. Therefore, we believe with regard to the definition under the act that the physical location does not dictate whether or not the equipment is under the control of the carrier.[62]

Interception capability plans

3.52 Proposed section 196 requires carriers to develop interception capability plans (ICP) and proposed section 195 sets out matters that must be included in the plan. AMTA submitted that proposed section 195:

> …significantly expands the factors that must be included in an Interception Capability Plan to include 'or a change in marketing or pricing of services'. AMTA is concerned that this section 195 will place a significant burden on carriers and CSPs [carriage service providers] to submit updated plans to the CAC each time a price change is made or marketing campaign is launched for each product service.[63]

3.53 Proposed paragraph 195(2)(f) and proposed subsection 195(4) would permit the Minister to determine additional matters that must be dealt with by an interception capability plan. Telstra expressed concern that this may allow the Ministerial determination to expand the scope of a carrier's interception capability obligations. It suggested that proposed subsection 195(4) should be amended to clarify that any matters specified by the Minister to be included in the interception capability plan should only relate to matters relevant to a carrier's interception capability obligations.[64]

Departmental response

3.54 In response to a question on notice, the Department rejected AMTA's view that proposed section 195 significantly expanded the matters that must be addressed in an interception capability plan:

---

62 *Committee Hansard*, 16 July 2007, p. 29.

63 *Submission 5*, p. 4. See also *Committee Hansard*, 16 July 2007, p. 16.

64 *Submission 9*, p. 4.

> These provisions are consistent with the current provisions in the Telecommunications Act. The guidance provided in the EM lists a number of factors that are likely, if implemented, to effect interception capability. The particular reference in the EM to changes in marketing or pricing of services is referring to instances where a carrier may offer free services or undertake major marketing campaigns with an expectation of substantially increasing their customer base, which is likely to have an impact on the ability to provide interception capability.[65]

3.55 In relation to Telstra's concern that proposed subsection 195(4) would permit the Minister to expand the matters to be dealt with by an interception capability plan beyond matters relevant to a carrier's interception capability obligations, the Department advised that:

> Any determination made by the Minister would necessarily be restricted to interception capability obligations as defined by the TIA Act or in accordance with any interception capability determinations made under proposed section 189 of the Bill.[66]

Exemptions

3.56 The Communications Access Coordinator (CAC) may grant exemptions to interception capability obligations under proposed section 192. Under proposed subsection 192(5), a carrier will be deemed to have an exemption where the carrier has applied in writing to the CAC and the CAC has not communicated a decision on the exemption application within 60 days of the application. Proposed subsection 192(6) provides that a deemed exemption only has effect until the CAC communicates to the carrier a decision on the exemption application.

3.57 Mr Michael Ryan of Telstra explained industry concerns with the operation of deemed exemptions:

> [F]rom our point of view the CAC has 60 days to consider an exemption application, and it is deemed after 60 days that you have got an exemption. The problem is that CAC can come back and say you no longer have that exemption, which then leaves us in a state of uncertainty as to what we do with those applications…It makes it very uncertain in terms of delivering advanced services to customers if there is no time line or dead end to the deemed period.[67]

3.58 AMTA argued that there should be a time limit of 180 days on the refusal of an exemption by the CAC under proposed subsection 192(6) unless the CAC could

---

65 *Answers to questions on notice*, 24 July 2007, p. 9.

66 *Answers to questions on notice*, 24 July 2007, p. 6.

67 *Committee Hansard*, 16 July 2007, p. 16.

establish that a demonstrated agency need for interception exists. Alternatively, AMTA suggested that this provision should be repealed.[68]

Departmental response

3.59 The Department advised the committee that, in practice, this issue was unlikely to arise as in the last two years no exemption application had required more than 60 days to reach a decision.[69] The Department also noted that:

> The situation is such that when any application for exemption is made, if it is a complex one—if there is a potential that an exemption will not be granted—we engage immediately with the provider so that there will be no potential surprises. We try to work with them to come up with a solution if we believe that they strongly need interception capability…[W]e seek that the providers ask for an exemption from their capability prior to the rollout of that service, because we do not want to slow down the rollout of services...We do not ask them to retrofit; we ask them to talk to us in advance of rolling out a service.[70]

Ministerial determinations

3.60 Telstra expressed concern about the Minister's power to make determinations in relation to interception capability under proposed section 189 and, in particular, the range of factors the Minister would be required to consider before making a determination. In response to a question on notice, Telstra stated that:

> …the section should be broadened to require the Minister to take into account the effect of the determination on the ability for new and innovative products to be introduced into the Australian market, as well as on existing products and services in the market (which includes the costs implications of making existing products/services compliant with the subsequent determination).[71]

3.61 Telstra explained further:

> In terms of new and innovative products and services, there may be various issues which make it extremely difficult or impossible to provide an interception capability. For instance, the Minister may issue a determination which requires industry to intercept a new or innovative product/service which may be hosted overseas where the overseas product vendor is unable to provide interception capability due to jurisdictional and/or technology

68 *Submission 5*, pp 3-4. See also Telstra, *Submission 9*, p. 3.

69 *Committee Hansard*, 16 July 2007, p. 30. See also Attorney-General's Department, *Answers to questions on notice*, 24 July 2007, p. 6.

70 *Committee Hansard*, 16 July 2007, pp 29-30.

71 *Answers to questions on notice*, 24 July 2007, p. 1.

> constraints. In this scenario, it may result in the new and innovative product/service not being able to be made available in Australia.[72]

Departmental response

3.62 The Department noted in evidence to the committee that the Minister would be required to consider the objects of the Telecommunications Act in making determinations in relation interception capabilities.[73] The EM explains that the objects of the Telecommunications Act include:

> …the provision of a regulatory framework that promotes the long term interests of end-users of carriage services, or of services provided by means of carriage services; and the efficiency and international competitiveness of the Australian telecommunications industry.[74]

Other issues

Network protection

3.63 Subsection 5F(2) and 5G(2) of the TIA Act currently provide the AFP with exemptions for the purposes of network protection and enforcing professional standards. Schedule 2, Items 11 and 12 would expand the current exemptions for the AFP to cover Commonwealth agencies (AFP, the Australian Commission for Law Enforcement Integrity and the Australian Crime Commission), security authorities (ASIO, the Department of Defence, the Department of Foreign Affairs and Trade) and eligible authorities of a state (police forces and integrity commissions), all of which are defined in subsection 5(1). These provisions will enable those agencies to monitor inbound and outbound communications for the purpose of enforcing professional standards and protecting their networks without the risk of breaching the TIA Act.[75]

3.64 However, the Inspector-General of Intelligence and Security (the IGIS) questioned whether the coverage to allow network administrators in certain agencies to protect network infrastructure is wide enough:

> While one can well understand the need for adequate protection of the agencies which directly protect obvious national security interests (ie Australia's defence, security, international relations or law enforcement), the question also arises as to whether there is other network infrastructure the protection of which is also of particular importance to Australia's interests.[76]

---

72 *Answers to questions on notice,* 24 July 2007, p. 1.

73 *Committee Hansard*, 16 July 2007, p. 28.

74 EM, pp 18-19.

75 EM, p. 42.

76 *Submission 14*, pp 3-4. See also Premier of Western Australia, *Submission 25*, pp 1-2.

Departmental response

3.65 The Department responded to a question on notice on this issue:

> The Department recognises that a number of agencies across the public and private sector need to ensure the security of their networks. The Department is also aware that changing technologies have made the existing provisions of the TIA Act increasingly at variance with the ways in which networks operate. As such, some legitimate network protection activities may result in technical breaches of the TIA Act.
>
> The current and proposed exemptions represent an interim measure to provide protection for those agencies that require the highest levels of network security. The Department is currently working on a permanent solution, which needs to take into consideration developing technologies and threats, systems administration procedures and workplace privacy.[77]

Oversight

3.66 The IGIS noted there may be a role for his office in monitoring authorisations to access prospective telecommunications data by ASIO officers. The IGIS suggested that these authorisations should be examined as part of the IGIS inspection program:

> This would involve periodic visits by my staff during which they would review all of the authorisations granted in the preceding period to ensure that there was sufficient justification and that requirements imposed by the Communications Access Coordinator under the proposed section 183 were met.[78]

Departmental response

3.67 The Department agreed with this suggestion and argued that the existing jurisdiction of the IGIS under the *Inspector-General of Intelligence and Security Act 1986* would allow him to perform this role:

> The IGIS has access to all of ASIO's records and staff and may enter the agency premises at any time. Importantly, the IGIS has the power to inquire into public complaints, conduct inquiries referred by Government, and initiate inquiries. The IGIS regularly undertakes compliance inspections of ASIO's records and reports on his findings in the IGIS Annual Report.
>
> Accordingly, the Department considers that the IGIS already has the necessary jurisdiction to oversight ASIO's use of the prospective data regime.[79]

---

77 *Answers to questions on notice*, 24 July 2007, pp 18-19.

78 *Submission 14*, p. 2.

79 *Answers to questions on notice*, 24 July 2007, p. 15.

Review

3.68 On the issue of periodic reviews of the TIA Act, OPC submitted:

> …the operation of the Interception Act should be subject to overall independent review including key stakeholder and public consultation at least every five years.[80]

Departmental response

3.69 The Department did not accept that the TIA Act should be the subject of a mandatory statutory review process:

> The Government does not agree to a requirement mandating formal review in this way. As the experience of the past ten years demonstrates, the legislation is subject to near constant operational review, leading to regular legislative amendments and associated Parliamentary and public scrutiny, including through Parliamentary Committee inquiries. This has included formal reviews of the regime governing interception and industry obligations to assist that were undertaken by Mr Pat Barrett, Mr Dale Boucher, Mr Peter Ford, Mr Tom Sherman and Mr Anthony Blunn, as well as five Senate Committee legislative inquiries. As such, any mandatory statutory review process is unnecessary.[81]

Committee view

3.70 The committee is satisfied that extensive consultation has occurred between the Department, the telecommunications industry, law enforcement and security agencies, and other interested parties. The committee, like many of these parties, welcomes the further implementation of recommendations made in the Blunn Review by the Bill, including establishment of a single comprehensive legislative regime dealing with access to telecommunications information.

3.71 The committee acknowledges that consultation between the government and the telecommunications industry is crucial to ensure that interception capabilities support the legitimate requirements of enforcement agencies without unduly impinging on the services provided by carriers and carriage service providers. While some submissions argued for formal requirements for consultation to be embedded in the Bill, the committee considers that continuation of the existing arrangements for consultation between government and industry are likely to be just as effective and considerably more flexible.

3.72 In the absence of any justification for the inclusion of CrimTrac in the definition of 'enforcement agency', the committee considers that CrimTrac should be removed from the definition. The inclusion of agencies in this definition provides

---

80 *Submission 19*, p. 6.

81 *Answers to questions on notice*, 24 July 2007, p. 5.

agencies with intrusive powers so the default position should be that agencies are excluded, unless a positive justification for their inclusion is forthcoming.

3.73 The committee believes that the suggestion that further guidance be provided to assist authorised officers in assessing the privacy implications of authorising access to prospective telecommunications data, as required by proposed subsection 180(5), is a constructive one. However, the committee is mindful of the Department's concerns that seeking to provide that guidance within the Bill is likely to be impractical given the range of circumstances confronting officers weighing these issues. The committee notes the Department's advice that privacy issues may be addressed through the determination of the CAC under proposed subsection 183(2) regarding the formal requirements for authorisations and notifications. The committee recommends that the CAC determination under that provision should address procedural requirements in relation to the consideration and documentation of privacy issues. In making this recommendation, the committee is mindful that proposed subsection 183(3) will require the CAC to consult with the Privacy Commissioner before making such a determination.

3.74 The committee supports the suggestion made by the IGIS that oversight of access to prospective telecommunication data by ASIO should form part of his regular inspection program. The committee notes advice from the Department that the existing powers of the IGIS would permit such inspections.

3.75 The Senate Legal and Constitutional Legislation Committee previously recommended an independent review of provisions inserted in the TIA Act by the Telecommunications (Interception) Amendment Bill 2006.[82] The committee believes that in light of the complexity of the legislation, its acknowledged impacts on privacy and the potential for significant changes in technology to substantially alter the reach and affect of provisions in the Act, an independent review of the TIA Act in the next five years is highly desirable. In particular, such a review would provide an opportunity to examine further the issues of:

- whether there is a need to define 'telecommunications data', or whether the distinction between 'content and substance' and other information and documents operates effectively;
- what impact further technological developments have on the operation of the TIA Act; and
- whether any of the obligations imposed on carriers and carriage service providers are unnecessarily hampering the efficient delivery of telecommunications services, including the introduction of new services.

3.76 The committee accepts the view of the government that it is unnecessary to amend the Bill to require such a review.

---

82 Senate Legal and Constitutional Legislation Committee, Provisions of the *Telecommunications (Interception) Amendment Bill 2006*, March 2006, Recommendation 25, p. 48.

Recommendation 1

3.77 The committee recommends that proposed paragraph 5(1)(m) of the Bill be deleted to remove CrimTrac from the definition of 'enforcement agency'.

Recommendation 2

3.78 The committee recommends that the determination of the Communications Access Coordinator under proposed subsection 183(2) address requirements for the consideration and documentation of privacy issues by authorised officers.

Recommendation 3

3.79 The committee recommends that the Inspector-General of Intelligence and Security incorporate into his regular inspection program oversight of the use of powers to obtain prospective telecommunications data by the Australian Security Intelligence Organisation.

Recommendation 4

3.80 The committee recommends that the Attorney-General's Department arrange for an independent review of the operation of the *Telecommunications (Interception and Access) Act 1979* within five years.

Recommendation 5

3.81 Subject to the preceding recommendations, the committee recommends that the Bill be passed.

Senator Guy Barnett
Chair

SUPPLEMENTARY REPORT WITH ADDITIONAL COMMENTS OF DISSENT BY THE AUSTRALIAN DEMOCRATS

1.1 The Democrats agree with a majority of the recommendations presented in the Chair's report.

1.2 We note the majority of submissions desire a single comprehensive legislative regime dealing with access to telecommunications information.

1.3 The Democrats note this Bill amends the *Telecommunications (Interception) Act 1979* to implement further recommendations from the August 2005 *Review of the Regulation of Access to Communications* by Anthony Blunn AO (the Blunn Review).

1.4 We believe the Bill, as introduced, does not adequately account for privacy considerations.

1.5 The operation of the Bill is in conjunction with other legislation which further reduces fundamental civil liberties of Australian citizens.

1.6 We believe a majority of the recommendations contained in the Chair's report will improve the Bill and lessen the potential for abuses of privacy but provide the following additions:

Definition of enforcement agency

1.7 The legislation gives enormous powers to law enforcement agencies to listen to the private conversations of Australians.

1.8 The Democrats believe that the definition of 'law enforcement agency' is too broad.

1.9 In particular we share the concerns raised in the inquiry that the Bill will grant new powers to the CrimTrac Agency to apply for stored communications warrants and to issue authorisations for access to historical 'telecommunications data'.

1.10 As Electronic Frontiers Australia state in their submission, CrimTrac is not a law enforcement agency authorised to conduct investigations into suspected offences except in limited circumstances related to spent conviction legislation.[1]

1.11 While we note the Department has stated that CrimTrac's functions do not include the investigation of any offences and therefore they will be ineligible to be issued with a stored communications warrant,[2] CrimTrac's functions could just as easily be expanded. We note that, in addition to providing criminal history checks, CrimTrac's functions have already been expanded into the area of DNA samples.

---

[1] Electronic Frontiers Australia, *Submission 6*, pp 4-5.

[2] *Committee Hansard*, 16 July, p. 10.

1.12 The Democrats do not consider, at this time, it is appropriate for CrimTrac to be included in the definition of a law enforcement agency.

Recommendation 1

1.13 The Democrats support the removal of CrimTrac from the definition of 'enforcement agency'.

Convergent technologies

1.14 There is a need to consider how best to respond to the fact that current and emerging communications technologies have resulted in a convergence of areas that have traditionally been separately regulated by federal or state government laws.

1.15 During the course of this inquiry various examples of converging technologies were discussed including, web browsing, downloading from the internet, entering chat rooms, sharing emails, taking digital photographs and video footage and playing MP3 files all from a mobile telephone. Questions were raised as to what information captured can properly be considered telecommunications data.

1.16 The best way to deal with these new technologies is to give certainty as to whether or not the information they produce can be categorised as telecommunications data. This is something which the Attorney-General's Department appears reluctant to do.

1.17 The Attorney-General's Department has stated that they are 'concerned about defining technology and call associated data now because the definition might be redundant in 12 months time'.[3] The Democrats are dissatisfied with this reason.

1.18 As a matter of public policy, it is desirable to clarify what is meant by telecommunications data now. If in a certain time period, albeit 6 or 18 months, that definition needs amending then this can occur. The absence of a clear definition should not be justified by an assertion that this will allow the law to remain current with technology.

1.19 With advances in technology it is important to clarify the scope of telecommunications data to reassure current and future users of new technologies that such communications may or may not be intercepted.

Recommendation 2

1.20 The Democrats will be amending any future Bill to define telecommunication data. The definition of telecommunications data will balance a desire to be technology neutral with a desire to protect certain citizen's lawful activities from disclosure to enforcement agencies

[3] *Committee Hansard*, 16 July 2007, p. 22.

Location Information

1.21 Location and identity are fundamental characteristics of telecommunications data. Location requires measurement. Identity requires classification and definition.

1.22 A by-product of locating a mobile telephone is the ability to locate with precision people. The Democrats acknowledge that this is a by-product, not an aim, of most telecommunications data collection. But it is a by-product that as the Law Council has noted in its submission which requires greater controls.[4]

1.23 Tom Wright, Information and Privacy Commissioner for Ontario, Canada, considered that location can:

> in essence become a personal identifier because geographical information systems technology enables the synthesis and analysis of information not possible with other information management systems. It can construct a very detailed picture of an individual's life, even without the use of their name, just by collecting and analysing data related to a specific location.[5]

1.24 The Democrats recommend that a person's mobile telephone phone should not be used as a surrogate tracking and tracing technology for people in the absence of any countervailing public interest, significant independent oversight and public reporting.

1.25 We favour access to location information only through a warrant.

Recommendation 3

1.26 The Democrats will be amending the Bill to ensure that real time data, in other words location information, can only be accessed by enforcement agencies with a warrant.

Time periods

1.27 As noted above, the Democrats believe in a requirement to allow mobile telephone location information to be disclosed under a warrant.

1.28 However, if this is not accepted by the government, then the Bill will allow mobile telephone location information to be disclosed under a written authorisation for a period of 45 or 90 days without the need to obtain a warrant.

1.29 The Democrats consider this time frame is excessive and should be limited.

Recommendation 4

1.30 Written authorisations to access mobile telephone location information should be limited to 14 days duration and should not be renewable unless during that 14 days information material to the investigation has been obtained which

---

[4] Law Council of Australia, *Submission 20*, p. 6.

[5] Tom Wright, *Geographic Information Systems*, at http://www.ipc.on.ca/english/pubpres/papers/gis.htm (accessed 31 July 2007).

suggests that continued interception would likely result in further material information. The duration of a renewed warrant should not exceed 20 days.

Public Interest Monitor

1.31 This Bill creates a new two tier access regime. The first tier encompasses the traditional access to existing telecommunications data. The second tier allows for access to future telecommunications data. The Bill also creates new controls over the existing access framework.

1.32 The Democrats view this Bill as a widening of the Commonwealth phone-tapping powers. 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.

1.33 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.

1.34 Queensland Premier Peter Beattie has also prepared telephone interception legislation to include a Public Interest Monitor.

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

Recommendation 5

1.36 The Democrats will amend the legislation to require enforcement agencies consult with the Public Interest Monitor (PIM) before they apply for an authorisation under the TIA Act.

Collection of telecommunications data which is necessary

1.37 Proposed sections 174 and 177 concern voluntary disclosures of telecommunications data to ASIO and enforcement agencies by employees of a carrier or carriage service provider.

1.38 The Democrats are concerned that an employee of a carrier or carriage service provider may volunteer more personal information than is necessary for ASIO and enforcement agencies to perform their functions. The reality is that employees of a carrier or carriage service provider when faced with a request or warrant from ASIO or an enforcement agency will be overly cooperative.

Recommendation 6

1.39 The Democrats propose that there be a positive obligation on the part of ASIO and the enforcement agency, where they suspect or have actual knowledge

that an employee of a carrier is volunteering personal information, to warn that employee that they are not legally obliged to disclose telecommunications data.

Conclusion

1.40 This Bill confirms privacy as a valued norm but does not do enough to protect Australians' private conversations and communications.

1.41 While legitimate law enforcement activities may in exceptional circumstances override a right to privacy the increasingly complex telecommunications environment exposes individuals to arbitrary interference.

1.42 The Democrats will be moving a number of amendments to this Bill to ensure there are greater protections afforded for telecommunications data.

Senator Stott Despoja
Australian Democrats

APPENDIX 1
SUBMISSIONS RECEIVED

Submission Number	Submittor
1	NSW Independent Commission Against Corruption
2	Optus
3	Department of Defence
4	Police Federation of Australia
5	Australian Mobile Telecommunications Association (AMTA)
6	Electronic Frontiers Australia Inc
6a	Electronic Frontiers Australia Inc
6b	Electronic Frontiers Australia Inc
7	NSW Ombudsman
8	Queensland Council for Civil Liberties
9	Telstra
10	New South Wales Council for Civil Liberties Inc (NSWCCL)
11	Vodafone Australia
12	Internode Systems Pty Ltd
13	Confidential
14	Inspector-General of Intelligence and Security
15	Attorney-General's Department
16	Privacy NSW
17	The Australian Privacy Foundation
18	Communications Alliance Ltd
19	Office of the Privacy Commissioner

20 Law Council of Australia

21 Western Australia Police Service

22 Corruption and Crime Commission of WA

23 Tasmania Police

24 South Australia Police

25 Premier of Western Australia

26 Internet Industry Association (IIA)

27 ACT Government

ADDITIONAL INFORMATION

1. Additional Information received from Professor Simon Bronitt and Mr James Stellios, Senior Lecturer, ANU College of Law, The Australian National University

2. Diagrams tabled by Attorney-General's Department, Telecommunications and Surveillance at public hearing in Canbera on Monday, 16 July 2007

3. Answers to Questions on Notice received from Michael Ryan, Member, Australian Mobile Telecommunications Association

4. Answers to Questions on Notice received from the Attorney-General's Department

APPENDIX 2

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

Canberra Monday, 16 July 2007

ALTHAUS, Mr Chris, Chief Executive Officer
Australian Mobile Telecommunications Association

BURGESS, Mr Mark, Chief Executive Officer
Police Federation of Australia

CURTIS, Mr Jonathan, Director
Attorney-General's Department

GRAHAM, Ms Irene Joy, Board Representative
Electronic Frontiers Australia Inc

KELLY, Ms Wendy, Assistant Director
Attorney-General's Department

LAMMERS, Federal Agent Rudi, Acting National Manager Border
Australian Federal Police

MARKEY, Mr Lionel Wayne, Director
Telecommunications and Surveillance Law Branch
Attorney-General's Department

RYAN, Mr Michael, Member
Australian Mobile Telecommunications Association

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

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