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.