INFORMATION, ANALYSIS
AND ADVICE FOR THE PARLIAMENT

INFORMATION AND RESEARCH SERVICES
PARLIAMENTARY LIBRARY

Bills Digest
No. 111 2003–04

Telecommunications (Interception) Amendment Bill 2004

ISSN 1328-8091

Inquiries

Members, Senators and Parliamentary staff can obtain further information from the Information and Research Services on (02) 6277 2404.

Information and Research Services publications are available on the ParlInfo database.
On the Internet the Parliamentary Library can be found at: http://www.aph.gov.au/library/

Published by the Information and Research Services, Parliamentary Library,
Department of Parliamentary Services, 2004.

INFORMATION AND RESEARCH SERVICES

Bills Digest
No. 111 2003–04

Telecommunications (Interception) Amendment Bill 2004

Peter Prince
Law and Bills Digest Group
23 March 2004

Contents

Telecommunications (Interception) Amendment Bill 2004

Date Introduced: 19 February 2004

House: House of Representatives

Portfolio: Attorney-General

Commencement: On the day after Royal Assent

Purpose

To amend the *Telecommunications (Interception) Act 1979* to:

- allow telecommunications interception in relation to new terrorism offences, offences involving dealings in firearms, and State and Territory cybercrime offences
- allow access to 'stored' or 'delayed access' communications (emails, text messages and voicemail) without an interception warrant
- allow recording of calls to ASIO public lines without any warrant
- amend the definition of 'interception' to accord with recent technological advances, and
- allow interception without notifying a telecommunications carrier in certain circumstances.

Background

Telecommunications interception

The Telecommunications (Interception) Act prohibits interception of 'a communication passing over a telecommunications system' except where this is necessary for the operation or maintenance of such a system or pursuant to an interception warrant.[1]

Types of interception warrants

Interception warrants can be issued for national security or law enforcement purposes.

ASIO's Director-General of Security can apply for an interception warrant relating to national security or foreign intelligence.[2] The Attorney-General may issue warrants for the interception of telecommunications where the subject of the warrant is reasonably suspected of engaging in activities prejudicial to security.[3] The Attorney-General can also issue interception warrants for the collection of foreign intelligence.[4]

In certain circumstances, ASIO's Director-General can issue a warrant for a limited period if waiting for a response from the Attorney-General would seriously prejudice national security.[5]

Law enforcement warrants can be obtained by Federal and State police and other government crime investigation bodies.[6] Applications for such warrants must be made to an 'eligible judge' or nominated member of the Administrative Appeals Tribunal.[7]

'Telecommunications service warrants' relate to a particular identified telecommunications service.[8] 'Named person warrants' apply to any telecommunication service that is used or likely to be used by a named individual.[9]

An application for an interception warrant can include a request that the warrant authorise entry onto specified premises.[10]

Interception warrants can only be issued for law enforcement purposes for the investigation of 'class 1' and 'class 2' offences. Class 1 offences include murder, acts of terrorism, kidnapping and narcotics offences.[11] Class 2 offences include offences punishable by imprisonment for life or a period of at least 7 years where the offender's conduct involves loss of life, serious personal injury, drug trafficking or serious fraud, bribery or corruption etc.[12]

An application by a law enforcement agency for an interception warrant must be accompanied by an affidavit containing prescribed information.[13] Before issuing either a 'class 1' or 'class 2' interception warrant, the judge or AAT member must consider whether sufficient information could be obtained by alternative methods. In the case of an interception warrant relating to a class 2 offence, the judge or AAT member must also take into account the extent to which the privacy of any person or persons would be interfered with, as well as the gravity of the conduct constituting the offence being investigated.[14]

Additional information must be supplied before a warrant can authorise entry on to premises.[15]

Interception versus search warrants

Police and other law enforcement authorities can obtain search warrants under various Commonwealth and State legislation.[16] While an interception warrant can only be issued for law enforcement purposes in relation to serious 'Class 1' and 'Class 2' crimes, a search warrant can be obtained for a broader range of offences. For example, under the Commonwealth *Crimes Act 1914* a search warrant can be obtained in relation to any Commonwealth criminal offence.[17] Instead of applying to a judge or member of the AAT as with interception warrants, search warrants can be obtained from a magistrate or a justice of the peace.[18]

While obtaining a search warrant is not automatic, the process has been designed to obtain physical evidence not gain access to communications (although it obviously allows access to the full range of items found on premises, including items such as computers, documents, letters etc). Consequently there is no specific requirement in the ordinary search warrant process to consider privacy issues.

Access to private communications, on the other hand, raises significant privacy issues, not least the rights of third parties whose communications may be accessed or about whom information may be revealed. Hence the Telecommunications (Interception) Act allows for such issues to be taken into account before an interception warrant is obtained, at least in relation to the less serious 'class 2' offences.[19] The Act also contains strict protocols on use and handling of information collected by means of interception warrants.[20] For example, section 67 allows use of intercepted information only for 'permitted purposes'. These 'permitted purposes' are set out in detail in section 5, and vary between the different Commonwealth and State agencies and bodies. The Act also contains extensive requirements both for keeping records of telecommunications interceptions and for annual reporting by State and Commonwealth authorities, including preparation of a detailed report for the Commonwealth Parliament.[21]

Parliament might also note that legislation governing the use of 'listening devices' (i.e. equipment able to 'record or listen to spoken words') lays down protocols similar to those in the Telecommunications (Interception) Act. Under the *Australian Federal Police Act 1979*, for example, a 'warrant for the use of a listening device' requires an application to a judge or member of the Administrative Appeals Tribunal, who is required to consider 'how much the privacy of any person would be likely to be interfered with by the use by officials of a listening device'.[22] In addition, 'listening device warrants' can only be obtained for 'class 1' and 'class 2' offences, which are similar to the offences in these categories in the Telecommunications (Interception) Act.

There is a considerable difference between the duration of ordinary search warrants and interception warrants. Under the Commonwealth Crimes Act, for example, a search warrant expires no later than a week after it is issued. In addition, the issuing officer must be satisfied that there are reasonable grounds for suspecting that relevant material will be on the premises subject to the warrant within 72 hours of the warrant being issued.[23] In

contrast, interception warrants issued for national security purposes have a maximum duration of six months.[24] Interception warrants issued to law enforcement agencies can remain in force for a period of up to 90 days.[25]

Number of interception warrants

The latest annual report[26] on the Telecommunications (Interception) Act states that during 2002-03, 3058 interception warrants were issued to law enforcement agencies, representing an increase of 22 per cent over the previous year.[27] Figures are not provided for the number of interception warrants granted on national security grounds or for the collection of foreign intelligence.

The number of criminal prosecutions commenced on the basis of information obtained through telecommunications interception warrants increased by 59 per cent in 2002-03, with a 31 per cent increase in the number of convictions obtained on the basis of lawfully obtained information.[28] This follows a similar increase in 2001-02.[29]

Commenting on these figures, the Attorney-General stated in March 2004 that:

> The increase in the number of interception warrants reflects the increasing use by targets of multiple services, mobile telephones and pre-paid services…The report shows that the use of telecommunications interception continues to be an important investigative tool which is producing positive results for law enforcement agencies.[30]

Democrat Senator Natasha Stott Despoja expressed concern about the increase in the number of 'renewal warrants' over the last two years, and observed that the number of warrants was not the same as the number of interceptions. While $25 million was spent in connection with the execution of warrants during 2002-03, there was a 'decrease in the number of arrests per warrant from the previous year, with only 50 arrests for every 100 warrants issued….More than 1,500 interception warrants did not result in any arrest.'[31] She commented:

> the picture this annual report creates is one of Australian law enforcement agencies undertaking more interceptions and spending more money on them but these not necessarily yielding more information relevant to criminal offences. It should be noted that these figures are restricted to law enforcement agencies only and do not incorporate the no doubt extensive investigative activity that is undertaken by Australia's intelligence agencies. I think this is a very worrying set of figures on an issue that is often overlooked. I hope that members of the public and people in this place will take a look at this report and recognise just how many Australians are literally being spied upon.[32]

For further background on telecommunications interception, see Bills Digest No. 121 of 2001-02[33] and Bills Digest No. 44 of 2003-04.[34]

Senate inquiry

On 3 March 2004 the Senate referred the provisions of the current Bill to the Senate Legal and Constitutional Legislation Committee, for report by 30 March 2004. Submissions were called for by 12 March 2004. The Committee's website notes that it 'is particularly interested in the appropriateness of the changes to the telecommunications interception regime proposed in the Bill, and whether previous concerns of the Committee have been addressed.'[35]

Senate report on 2002 Bill

In May 2002 the Senate Legal and Constitutional Legislation Committee reported on the Telecommunications Interception Legislation Amendment Bill 2002. As with the 2004 Bill, the 2002 Bill proposed to allow access to 'stored' or 'delayed access' communications without an interception warrant. However the proposal was removed from the final version of the 2002 Bill after the Committee's report[36] recommended that an interception warrant should be required for access to such communications.

Concerns expressed to the Committee focussed on the ability to access emails, text messages and similar communications 'stored' on equipment operated by an internet service provider (ISP) before being delivered to the intended recipient. In its original form the 2002 Bill would have allowed access without an interception warrant to such communications while they were in this temporary 'stored' mode. Instead of an interception warrant, some other form of lawful authority such as an ordinary search warrant could be used to gain access. While the Attorney-General's Department and the Australian Securities and Investment Commission expressed support for the proposal, other individuals and groups, including both the Federal and NSW Privacy Commissioners, were opposed. According to the Federal Privacy Commissioner:

> There seems to be little justification for reducing the privacy protection of a communication as intimate as a voice mail message or SMS, in comparison with a 'live communication' simply because the transmission of the former is temporarily delayed.[37]

Electronic Frontiers Australia told the Committee that allowing access to stored communications on an ISP's premises by way of a search warrant where the intended recipient is unaware this is being done would create 'a whole secret surveillance society where there is absolutely no chance of review of any abuse of power':

> All of the protections that come with the interception legislation go out the door in relation to messages in transit. Instead of…a warrant only able to be issued by the AAT, you are going to have a situation where police officers can get a search warrant to go into ISP premises and check what e-mails are being sent to you, before you have even received them, and so on.[38]

The current Bill and access to stored communications

In his second reading speech introducing the current Bill, the Attorney-General said that proposed amendments to the Telecommunications (Interception) Act allowing access to stored communications without an interception warrant 'differ from those previously introduced, and address concerns expressed during consideration of the earlier amendments' by the Committee.[39]

The Explanatory Memorandum for the 2004 Bill explains that there will be three circumstances in which a stored communication will be deemed not to be 'passing over' a telecommunications system, and where interception will therefore require only an ordinary search warrant or similar rather than an interception warrant:

- when the communication is received by the intended recipient or a person with the authority of the intended recipient

- when it is accessed by an ASIO or law enforcement officer after it has been received by the intended recipient and without using an ISP or other remote service, and

- when it is accessed by an ASIO or law enforcement officer using equipment the intended recipient could have used.[40]

The Explanatory Memorandum says that an officer could not use an ordinary search warrant to access stored emails held on an ISP's server until 'after the communication has been accessed by the intended recipient'. It notes that 'an officer could therefore obtain a copy of the message from the ISP, but could not connect to the ISP to access the account directly'. Similarly, in the case of voicemail, normally stored by the service provider on its network until the subscriber dials in to retrieve the message, the Explanatory Memorandum explains that an ASIO officer or a law enforcement officer could only use an ordinary search warrant to obtain the message 'after the communication has been accessed by the intended recipient'.[41]

The Explanatory Memorandum states that because text messages via mobile telephones do not involve use of an ISP or remote access, the issue of 'intercepting' such communications before they have been received on the intended recipient's equipment does not arise.[42]

Reaction to 2004 Bill

Electronic Frontiers Australia's initial reaction to the current Bill was favourable. Noting that an interception warrant would be required to access messages stored by an ISP or other service provider and not yet delivered to the intended recipient, the organisation's executive director, Irene Graham, said that it 'looks like they've done it properly this time….The interception warrant provides much more protection for people's privacy than

an ordinary search warrant'. Ms Graham stated, however, that EFA's board was still examining details of the proposed amendments.[43]

The NSW Council for Civil Liberties was less convinced. While agreeing that the new provision resolved technical problems about the receipt of emails, the Council said the 2004 Bill provided broader access to communications and reduced personal privacy for people 'who may be innocently caught up in an investigation'. President of the Council, Cameron Murphy, was concerned that the amendments in the current Bill would make telecommunications interception warrants similar to named-person warrants allowing interception of any communication sent to a particular person:

> There's a different standard for that….If you're going to protect people's privacy, our argument is it should be more specific; for example to intercept communications only between the subject of the warrant and other people involved in an investigation.[44]

New 'class 1' and 'class 2' offences

The Telecommunications (Interception) Act currently includes general 'acts of terrorism' as a 'class 1' offence in relation to which law enforcement agencies can seek an interception warrant.[45] The Bill will add the specific terrorism offences recently included in the Commonwealth *Criminal Code* to the definition of 'class 1' offence in the Act.

The amendment will allow law enforcement officers as well as ASIO officers to apply for interception warrants to investigate terrorist activities in Australia.

For background on the new terrorism offences, see Bills Digest 126 2001-02, Security Legislation Amendment (Terrorism) Bill 2002 [No. 2].[46]

The Bill also adds various 'cybercrime' offences and 'dealings in firearms and armaments' to the list of 'class 2' offences for which law enforcement agencies can seek an interception warrant under the Telecommunications (Interception) Act.

Notifying telecommunications carriers

Under section 15 of the Telecommunications (Interception) Act, the Director-General of ASIO must cause the managing director of a telecommunications carrier to be informed of the issue of a warrant allowing interception of communications passing over the carrier's network. A copy of the warrant must also be provided. The Bill proposes to drop this requirement in the case of interception warrants issued to ASIO where interception will not require action by the carrier. A similar amendment is not proposed in the case of interception warrants issued to law enforcement agencies. Under section 60 of the Act, law enforcement agencies will still be required to inform telecommunications carriers when communications on their networks are intercepted, even where no action by the carrier is needed.

Main provisions

New offences for interception purposes

Item 1 (of Schedule 1) adds specific terrorism offences now included in the Commonwealth *Criminal Code*[47] to the definition of 'class 1 offence' in **subsection 5(1)** of the Telecommunications (Interception) Act. **Items 3 and 4** add further offences to the definition of 'class 2' offence in section 5D of the Act, namely 'dealings in firearms and armaments' (replacing 'armament dealings') and cybercrime offences under various Commonwealth, State and Territory laws.

New definition of 'interception'

Items 5-9 amend the definition of 'interception' of a communication in **section 6** of the Telecommunications (Interception) Act to include not only 'listening and recording' but also 'reading or viewing'. As the Explanatory Memorandum notes, this broader definition is more appropriate for modern forms of communication such as emails and images for which the concepts of 'listening' and 'recording' are not directly applicable. The effect is to extend the protection in **section 7** of the Act against interception without lawful authority to cover these additional modes of accessing a communication.

Communications to publicly-listed ASIO numbers

Item 10 proposes to add **new subsections 6(3) and 6(4)** to the Telecommunications (Interception) Act providing that listening to, recording, reading or viewing telephone calls to publicly listed ASIO numbers by a person lawfully engaged in duties related to handling such communications will not constitute 'interception' and will not require a warrant.

The Explanatory Memorandum notes that the amendment 'is limited to calls made to ASIO and does not extend to allowing the recording of calls made from ASIO'.[48]

Access to stored communications

Item 10 will also add new subsections **6(5) to 6(7)** to the Telecommunications (Interception) Act specifying three circumstances in which a 'stored communication' (such as email, text messages and voicemail) will not be 'passing over' a communications system, allowing it to be accessed without an interception warrant:

- **Proposed paragraph 6(7)(a)** provides that a stored communication is not 'passing over' a telecommunications systems *'when it is accessed by* or with the authority of the intended recipient' (emphasis added). This appears intended to perform the same function as existing **subsection 6(2)** which provides that an unlawful 'interception'

does not occur if the listening or recording is carried out by a person lawfully on premises (in other words, using your own telephone etc).

Possible drafting error: The phrase 'when it is accessed by' has more than one meaning. It can mean *'if or where'* a communication is accessed by the lawful recipient. It can also mean *'at the same time'* as such access. The latter meaning would allow ASIO or law enforcement agencies to use an ordinary search warrant or other lawful authority to access any 'stored communication' (email, text message, voicemail) if this occurs 'when it is accessed by', i.e. at the same time that the intended recipient accesses the communication.

- **Proposed paragraph 6(7)(b)** will allow authorities to use an ordinary search warrant or similar to access any stored communication *after it has been accessed* by the intended recipient, provided this is done without using an ISP or other remote service.
  - However an ISP or other remote service can be used in the process of gaining access if this is 'merely for the purpose or an incidental result of' 'turning on equipment', 'obtaining power to operate equipment' or 'any other action prescribed by regulations…'.
- **Proposed paragraph 6(7)(c)** will allow ASIO or law enforcement agencies to access emails or text messages without needing to obtain an interception warrant, if this is done using 'any or all of the equipment which the intended recipient could have used', including 'in combination with other equipment', provided an ISP or other remote service is not used (although with the same exceptions as in **paragraph 6(7)(b)).**
  - This appears to allow agencies to use a search warrant or other form of lawful authority to 'intercept' emails and text messages *before* the intended recipient is aware of such communications, if they are already on the intended recipient's equipment, or become 'stored' there as an incidental result of the agencies turning on the equipment etc. Given the amount of emails many people receive, a particular message may not be noticed by the intended recipient, or if it is noticed, its significance may not be apparent. In either case, the recipient may not have read or viewed the message before ASIO or law enforcement officers gain access to the computer using an ordinary search warrant.
  - As well as emails, the Explanatory Memorandum indicates that **paragraph 6(7)(c)** could be used to access text messages before they are read by the intended recipient.[49] Seizure of a person's mobile phone under an ordinary warrant or other form of lawful authority would allow authorities to turn it on and view any text messages that are received before the intended recipient has read or is even aware of these.
  - The Explanatory Memorandum says it is not possible to access emails stored on a server that have not yet arrived on the intended recipient's computer under

paragraph 6(7)(c) since this requires 'dialling in' to the ISP or taking advantage of an 'always on' internet connection, which the provision does not permit.[50] This is inconsistent with a strict reading of the Bill. On its terms, proposed **paragraph 6(7)(c)** allows 'use of a telecommunications service' (such as an 'always on' internet connection) if this is merely 'an incidental result' either of 'turning on equipment' or 'any other action prescribed by regulations'. Personal computers can be configured so that emails automatically arrive via an 'always on' internet connection when the computer is turned on. As with text messages that arrive on a seized mobile phone, gaining access to computers set up in this way under an ordinary search warrant would allow arriving emails to be read by security or law enforcement authorities. Contrary to the explanation in the Explanatory Memorandum, **paragraph 6(7)(c)** as currently drafted permits access to such emails without an interception warrant.

- If, however, the Explanatory Memorandum is correct and **paragraph 6(7)(c)** prevents access without an interception warrant to emails that arrive through an 'always on' internet connection when a computer is turned on, security and law enforcement agencies would face a dilemma. If in the process of turning on a computer to which access has been granted under an ordinary search warrant, email messages arrive by virtue of an 'always on' internet connection, the authorities would be required (according to the Explanatory Memorandum) to ignore the relevant emails until they have obtained an interception warrant.

Notifying communications carriers

Items 13 and 15 amend **section 15** of the Telecommunications (Interception) Act to provide that where interception does not require action by a telecommunications carrier or its employees, the Director-General of ASIO does not need to advise the carrier that a warrant has been issued allowing interception of communications passing over the carrier's system.

Concluding comments

Access to stored communications without an interception warrant

Parliament needs to consider whether access by ASIO or law enforcement authorities to stored communications (emails, voicemail and text messages) without the knowledge of the recipient or sender should be allowed without adhering to protocols for intercepting private communications of the type laid down in the Telecommunications (Interception) Act.

Modern forms of electronic communication such as text messages and emails were not envisaged when the Telecommunications (Interception) Act was enacted 25 years ago. Yet reliance on such forms of communication is substantial in 2004 and will plainly increase. Use of interception warrants is also increasing significantly. In 1992-93, 527 interception warrants were issued to law enforcement agencies;[51] ten years later this had increased to 3058.[52]

The Telecommunications (Interception) Act is designed for the particular issues raised by official access to private communications passing over telecommunications systems. The 1994 Barrett report[53] noted that the Act conforms to privacy principles in the Commonwealth *Privacy Act 1988*. Indeed, the report noted that the Telecommunications (Interception) Act 'and the administrative procedures that have been established under it, afford a higher standard of privacy protection than is required by the [privacy] principles'.[54]

According to the Government, the amendments in the Bill relating to stored communications 'are intended to legislatively clarify the application of the Act to modern means of telecommunication'.[55] In providing that a communication is not 'passing over' a telecommunications service when accessed in a particular way, the Bill aims to 'achieve certainty in the scope and application of the Act'.[56] The Attorney-General stated that

> the amendments achieve an appropriate balance between protecting communications passing over the telecommunications system and the need for accessibility in the investigation of serious crime and security matters.[57]

Clarification of the circumstances in which an interception warrant is required will benefit the operations of security and law enforcement agencies. The current Bill restricts access by security and law enforcement agencies to electronic communications sitting on a server or some other form of remote service without an interception warrant. This addresses concerns expressed about the 2002 Bill (although see comments above re proposed **paragraph 6(7)(c)**). The Bill also describes circumstances in which a stored communication is taken not to be 'passing over' a telecommunications system where access by these agencies therefore requires some form of lawful authority but not an interception warrant.

The fundamental issue, however, is what privacy regime should apply for emails, text messages and voicemail, as well as for similar forms of electronic communication that may be developed in the future. Should official access to private communications using new forms of electronic technology be allowed outside the type of protocols in the Telecommunications (Interception) Act simply because the communications have reached a point in their transmission where they are deemed by the Bill to be no longer 'passing over' a telecommunications system?

For example, should ASIO or law enforcement officers be able to access a text message or email without the knowledge of the intended recipient with an ordinary search warrant

(thus avoiding the need to comply with the pre-requisites and procedures in the Telecommunications (Interception) Act) just because the message has arrived on the recipient's computer or mobile phone, but before the recipient has necessarily read or viewed the message or is even aware of its existence?

If an ordinary search warrant is all that is required, electronic communications will be treated similarly to traditional methods of communication, eg ordinary mail. Security and law enforcement agencies could gain access to private electronic communications in relation to a broad range of possible offences, not merely for investigation of the more serious 'class 1' and 'class 2' offences as required under the Telecommunications (Interception) Act. Lesser scrutiny requirements also apply.

The apparent drafting error in proposed **paragraph 6(7)(a) –** which on a strict reading would allow access to stored communications without an interception warrant by whatever means if this occurs 'at the same time' as access by the intended recipient – needs to be remedied. The apparent inconsistency between the terms of proposed **paragraph 6(7)(c)** – allowing access without an interception warrant to emails on a server if this is an incidental result of turning on a computer with 'always on' internet access – and the suggestion in the Explanatory Memorandum[58] that such access would not be permitted, should also be addressed.

Notifying Telecommunications Carriers

The proposed amendment to **section 15** of the Telecommunications (Interception) Act removing the requirement for the Director-General of ASIO to inform a carrier where interception does not require action by the carrier or its employees raises a further policy issue for Parliament to consider, namely should telecommunications carriers be informed in all cases when communications passing over their networks are intercepted? Parliament might note that while the Bill proposes to drop the notification requirement in such circumstances for interceptions by ASIO, a similar amendment is not proposed under **section 60** of the Act for interceptions by law enforcement agencies. Law enforcement agencies will still be required to inform telecommunications carriers in all cases when communications on their networks are intercepted. The rationale for removing this requirement for ASIO but retaining it for law enforcement agencies is not set out in the Attorney-General's second reading speech or in the Explanatory Memorandum.

Endnotes

1 Telecommunications (Interception) Act section 7.

2 Sections 9, 9A, and 11A–11C.

3 Sections 9 and 9A.

4 Sections 11A-11C.

5 Section 10.

6 The following agencies can apply for and obtain interception warrants for the purpose of law enforcement:

- the Australian Federal Police
- the Australian Crime Commission, and
- an 'eligible authority' of a State or the Northern Territory in respect of which a Ministerial declaration is in force. As at 30 June 2003, Ministerial declarations were in force for the Victorian, NSW, South Australian and Western Australian police services, the NSW Crime Commission, the NSW Independent Commission Against Corruption (ICAC), the NSW Police Integrity Commission and the Western Australian Anti-Corruption Commission. See *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2003*, p.10. Ministerial declarations are disallowable instruments under the Act (section 36). Some other agencies that are 'eligible authorities' under the Act but for whom no Ministerial declaration is in force can obtain lawfully intercepted information from intercepting agencies when that information relates to their own investigations (section 68).

7 Telecommunications (Interception) Act sections 6D, 6DA and 39.

8 Sections 9, 11A, 45, 46, 48.

9 Sections 9A, 11B, 45A, 46A.

10 Section 48.

11 Section 5.

12 Section 5D.

13 Section 42.

14 Sections 46 and 46A.

15 Section 48.

16 See eg *Crimes Act 1914* (Cth) Part 1AA, *Search Warrants Act 1985* (NSW).

17 *Crimes Act 1914 (Cth)* Part 1AA. A search warrant can be issued where the issuing officer has reasonable grounds for suspecting that there is, or will be within 72 hours, any 'evidential material' on the premises (subsection 3E(1)). 'Evidential material' is defined as a thing relevant to a summary or indictable offence (subsection 3C(1)).

18 Or another person employed in a court authorised for this purpose. Crimes Act sections 3C, 3E.

19 Sections 46 and 46A.

20 Part VII – Dealing with intercepted information

21 Parts VIII and IX.

22 Australian Federal Police Act section 12G.

23 *Crimes Act 1914* (Cth) section 3E.

24 Telecommunications (Interception) Act subsections 9B(3) and 11D(2).

25 Section 49(3).

26 http://www.ag.gov.au/www/agdHome.nsf/AllDocs/6EDC9CC0FC414ED6CA256E45000023F7?OpenDocument

27 *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2003*, p. 17.

28 ibid., p. 34.

29 *Telecommunications (Interception) Act 1979. Report for the year ending 30 June 2002*, p. 30.

30 Attorney-General, Press Release 9 March 2004, No 26/2004.

31 *Senate Hansard*, 9 March 2004, p. 20834.

32 ibid.

33 http://www.aph.gov.au/library/pubs/bd/2001-02/02bd121.pdf.

34 http://www.aph.gov.au/library/pubs/bd/2003-04/04bd044.htm.

35 http://www.aph.gov.au/senate/committee/legcon_ctte/tel_intercept04/index.htm.

36 http://www.aph.gov.au/senate/committee/legcon_ctte/terrorism/report/report.pdf.

37 Senate Legal and Constitutional Legislation Committee, *Report into Telecommunications Interception Legislation Amendment Bill 2002 and other Bills*, May 2002, p. 64.

38 ibid, pp. 63-4.

39 Hon. Philip Ruddock MP, Second Reading Speech, *House Hansard* 19 February 2004, p. 25230.

40 Explanatory Memorandum, p. 6.

41 ibid, p. 8.

42 ibid, p. 7.

43 'Mixed views on cops' email power', *The Australian*, 24 February 2004, p. 34.

44 ibid.

45 Subsection 5(1).

46 http://www.aph.gov.au/library/pubs/bd/2001-02/02bd126.htm. Some amendments were made to the Bill during its passage that are not reflected in the Digest.

47 Divisions 72, 101, 102 and 103.

48 Explanatory Memorandum p. 5.

49 ibid, p. 7.

50 ibid, p. 8.

51 *Review of the long term cost effectiveness of telecommunications interception*, March 1994, p. 60.

52 *Telecommunications (Interception) Act 1979 Report for the year ending 30 June 2003*, p. 17.

53 *Review of the long term cost effectiveness of telecommunications interception*, March 1994.

54 ibid, p. 56.

55 Explanatory Memorandum p.5.

56 Hon. Philip Ruddock MP, Second Reading Speech, *House Hansard* 19 February 2004, p. 25230.

57 ibid.

58 Explanatory Memorandum, p.8.