INFORMATION, ANALYSIS
AND ADVICE FOR THE PARLIAMENT

INFORMATION AND RESEARCH SERVICES
PARLIAMENTARY LIBRARY

Bills Digest
No. 153 2003–04

Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

ISSN 1328-8091

This paper has been prepared for general distribution to Senators and Members of the Australian Parliament. While great care is taken to ensure that the paper is accurate and balanced, the paper is written using information publicly available at the time of production. The views expressed are those of the author and should not be attributed to Information and Research Services (IRS). Advice on legislation or legal policy issues contained in this paper is provided for use in parliamentary debate and for related parliamentary purposes. This paper is not professional legal opinion. Readers are reminded that the paper is not an official parliamentary or Australian government document. IRS staff are available to discuss the paper's contents with Senators and Members and their staff but not with members of the public.

Inquiries

Members, Senators and Parliamentary staff can obtain further information from the Information and Research Services on (02) 6277 2646.

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 Information and Research Services, Parliamentary Library,
Department of Parliamentary Services, 2004.

INFORMATION AND RESEARCH SERVICES

Bills Digest
No. 153 2003–04

Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

Peter Prince
Law and Bills Digest Section
3 June 2004

Contents

Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

Date Introduced: 27 May 2004

House: House of Representatives

Portfolio: Attorney-General

Commencement: The day after Royal Assent

Purpose

To exclude 'stored communications' (defined broadly to include electronic messages located on a computer, internet server or other equipment, and whether read or unread) from the controls on interception of communications in the *Telecommunications (Interception) Act 1979* for a period of 12 months while a review of the Act is conducted.

Background

Detailed background on the telecommunications interception regime in Australia is contained in Bills Digest No 111 of 2003-04[1] concerning the Telecommunications (Interception) Amendment Bill 2004, introduced in February 2004 and enacted on 27 April 2004 (the 'February Bill').

The introduction of the current Bill follows the Government's withdrawal of amendments relating to 'stored' or 'delayed access' communications (emails, text messages and voicemail) in the February Bill. That Bill proposed amendments to the Telecommunications (Interception) Act allowing access without an 'interception warrant' to stored communications in certain circumstances. In specified situations, interception of such communications by ASIO or law enforcement agencies could be conducted using an ordinary search warrant or similar, and the protocols for intercepting private communications laid down in the Act would not apply.

The Government withdrew its amendments after a report[2] by the Senate Legal and Constitutional Affairs Legislation Committee revealed disagreement between government agencies over the current operation of the Telecommunications (Interception) Act in relation to interception of stored communications.

The major issue was whether the current Act requires law enforcement agencies to obtain an interception warrant to access unread emails stored at an intermediate point before they have been delivered to the intended recipient. The Australian Federal Police (AFP) cited advice from the Commonwealth Director of Public Prosecutions that section 3L of the *Crimes Act 1914* (as amended by the *Cybercrime Act 2001*) allows officers acting under an ordinary search warrant to access both read and unread emails found on a computer, including any stored 'remotely', for example on equipment operated by an internet service provider (ISP). According to the AFP:

> the intention of 3L was clearly to allow access to stored communications held remotely under the auspices and accountabilities of the search warrant regime.[3]

Contradicting the AFP's advice, the Attorney-General's Department submitted a legal opinion from the Commonwealth Solicitor-General which said that the current operation of the Telecommunications (Interception) Act:

> would…preclude a law enforcement agency from accessing an email stored at an intermediate point in transit, such as an ISP, in circumstances where that communication has not previously been accessed by the intended recipient, without a telecommunications interception warrant.[4]

The amendments proposed by the Government in the February Bill assumed that the current law required an interception warrant to access stored communications and were intended to introduce exceptions to this requirement. The AFP noted that if the amendments were enacted without an exemption for law enforcement agencies seeking to use an ordinary search warrant under section 3L of the Crimes Act, there would be 'severe operational difficulties'.[5]

In its report the Committee said it was 'most concerned' by the disagreement between the AFP and the Attorney-General's Department over the current state of the law relating to stored communications and the proposed amendments in the February Bill. It recommended that parliamentary consideration of the amendments be deferred until:

> Parliament is informed of agreement between the Attorney-General's Department and the AFP on the current operation of the TI regime, and how it will operate under the [proposed amendments].[6]

In his second reading speech the Attorney-General, Mr Ruddock, noted that the amendments proposed in the current Bill 'address concerns expressed by the AFP in relation to operational difficulties posed by the current interception regime'.[7]

2002 Bill

The current Bill is the third attempt by the Government to exempt 'stored communications' in whole or in part from the protections and protocols of the Telecommunications (Interception) Act.

In the Telecommunications Interception Legislation Amendment Bill 2002, the Government proposed to allow access to most stored or delayed access communications without an interception warrant. After concerns about the effect on privacy of email communications were raised with the Senate Legal and Constitutional Affairs Legislation Committee, the proposal was removed from the final version of the 2002 Bill. According to the Federal Privacy Commissioner, for example:

> 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.[8]

The amendments to the Telecommunications (Interception) Act proposed in the February Bill were drafted with criticisms of the 2002 Bill in mind. In his second reading speech for the February Bill, Mr Ruddock said that it addressed 'concerns expressed during consideration of the earlier amendments' by the Senate Legal and Constitutional Affairs Legislation Committee.[9]

Temporary effect of the current Bill

For a temporary period of 12 months, the current Bill will introduce an exclusion from the Telecommunications (Interception) Act for 'stored communications' which is broader in scope than that proposed in either the 2002 Bill or the February Bill.

The earlier Bills proposed – for the purpose of the prohibition in subsection 7(1) of the Act against interception of communications 'passing over' a telecommunications system - that in certain situations emails, text messages, voice mail etc be deemed to be no longer 'passing over' any such system. In other words, only part of the category of messages classed as 'stored communications' would be outside the Telecommunications (Interception) Act. In the February Bill, for example, an interception warrant would still be required to access stored emails held on an ISP's server that had not been read by the intended recipient.

The current Bill instead proposes that the prohibition in subsection 7(1) of the Telecommunications (Interception) Act not apply to 'stored communications' generally, with limited exceptions. The explanatory memorandum notes, for example, that an 'interception warrant will not be required to intercept stored e-mail',[10] which would include emails stored on an ISP's server, whether received by the intended recipient or not.

Review of Telecommunications (Interception) Act

Mr Ruddock explained in the second reading speech that the measures in the Bill 'represent immediate and practical steps to address the operational issues faced by our law enforcement and regulatory agencies'.[11] There was also a need, however, for a 'more

comprehensive review of access to stored communications and the contemporary relevance of Australia's interception regime'. Mr Ruddock observed that:

> When the act was drafted almost 25 years ago, the Australian telecommunications systems consisted largely of land based services carrying live telephone conversations. The act was therefore built around a core concept of communications passing over a telecommunications system. While this concept is technologically neutral, its application has proven more difficult to modern communications services…such as voice mail, email and SMS messaging.[12]

Mr Ruddock announced that he had therefore asked the Attorney-General's Department to conduct a 'comprehensive review' of the Telecommunications (Interception) Act, and to report back to him before the amendments in the Bill cease to have effect 12 months from the date of commencement.

Main Provisions

Schedule 1 Item 2 adds **new subsection 6E(3)** to the Telecommunications (Interception) Act which provides that a reference in the Act to 'lawfully obtained information' does not include information obtained by intercepting a 'stored communication', as long as the interception occurs within 12 months of the commencement of the current Bill. As the explanatory memorandum notes, the effect is to exclude such information from the restrictions on use and disclosure of intercepted material set out in Part VII of the Act.[13] Section 63 of the Act, for example, contains a general prohibition against 'lawfully obtained information' (i.e. information obtained without an interception warrant) being communicated to another person or being used in evidence in a proceeding.[14] Under the current Bill, information obtained from interception of 'stored communications' will not be covered by this prohibition.

Item 3 inserts **new paragraph 7(2)(ad)** to the Telecommunications (Interception) Act which provides that the prohibition in subsection 7(1) against interception of telecommunications without an 'interception warrant' does not apply to 'stored communications' intercepted in the 12 month period following commencement of the Bill. The explanatory memorandum explains that the practical effect of this item is that:

> it will no longer be necessary to obtain a telecommunications interception warrant, or to rely on some other exception to the prohibition against interception, in order to intercept a stored communication.[15]

Lawful access to the communication or the equipment on which it is stored will still be required. The explanatory memorandum notes that this could be through the consent of the intended recipient, under an ordinary search warrant or using the right to lawful access of a network owner or administrator.[16]

Item 4 defines inserts **new subsection 7(3A)** in the Telecommunications (Interception) Act which defines 'stored communication' for the purpose of the Act as 'a communication that is stored on any equipment or any other thing' with the exception of a 'voice over Internet protocol' communication or any other communication stored on a 'highly transitory' basis. The **note** to **item 4** cites 'momentary buffering (including momentary storage in a router in order to resolve a path for further transmission)' as an example of storage of a 'highly transitory' nature.

Concluding Comments

Review of Telecommunications (Interception) Act

The Government's intention to review 'the contemporary relevance of Australia's current interception regime' is a first step towards resolving the multitude of sometimes competing legal requirements concerning access to private information. As the digest[17] for the Surveillance Devices Bill 2004 noted:

> If the [Surveillance Devices] Bill is passed it will add to the number of different warrants that are available under different statutes covering similar situations. There will also be new categories of information and associated rules for using and communicating it (for instance, three categories of information under the Bill in addition to information covered by Part VII of the TI Act). There are also different accountability regimes under the Bill and the TI Act. Further, entirely different rules apply to search warrants under section 3L of the Crimes Act.
>
> Parliament may wish to consider whether this combination of fragmentation and complexity will create unacceptable difficulties for both law enforcement agencies and people who are placed under surveillance, whose telecommunications are intercepted and whose computers may be accessed.[18]

In this context it would be useful for Parliament to be informed of, and have the opportunity to comment on, the terms of reference for the proposed review. A review of the Telecommunications (Interception) Act and its adequacy in relation to new forms of communications technology should be a central part of any review, but as the above quote indicates, may not be sufficient in itself. Especially given disagreement between key government agencies about operation of current laws, a broader review appears to be needed to look at the range of situations in which some form of warrant or other lawful authority is required for access to private information, the adequacy of the various legislation covering such situations, and options for simplifying and clarifying the existing legal regime.

Any such review should be tabled in Parliament, subject to appropriate arrangements to safeguard sensitive operational information. This would allow Parliament to assess both

the adequacy of the review and the adequacy of any legislation proposed as a response to the review.

Timeframe for review and scope for consultation

It might be queried whether the 12 months allowed by the Government will be sufficient time for the intended review to be completed, especially if broader aspects of the legal regime covering obtaining of private information are included. This appears to be a relatively short time to conduct a review (including appropriate consultation), report to the Government and draft resulting legislation to take the place of the provisions in the current Bill.

The Senate Legal and Constitutional Affairs Legislation Committee called for Parliament to be informed of agreement between the AFP and the Attorney-General's Department about the practical effect of relevant legislation before any further consideration of exempting 'stored communications' from the interception regime in the Telecommunications (Interception) Act. In view of the privacy (as well as operational) issues that are involved, which have led to the defeat of previous Government proposals to introduce such an exemption, it would be useful if the review process included at least a consultation draft for all interested parties to comment on. It is not only law enforcement and national security agencies that have an interest in this issue, but also those with privacy responsibilities (such as the Federal Privacy Commissioner and State and Territory counterparts) as well as a wide range of organisations involved in or dependant on the electronic communications industry.

The approach in the current Bill

The protections in the Telecommunications (Interception) Act were specifically designed to balance law enforcement and national security needs with privacy concerns in relation to personal communications. As the Government has now identified, a key issue is how the legal regime in the Telecommunications (Interception) Act (and in other legislation) should be adapted for new communications technology not envisaged when the Act was enacted 25 years ago.

An issue for Parliament is whether – despite the time limit of 12 months on operation of the amendments in the current Bill – the approach proposed by the Government effectively pre-empts any review. If an exemption for 'stored communications' from the interception regime in the Telecommunications (Interception) Act is in place for a year, will it be impractical to institute some other legal regime, whatever the outcome of any review?

This is a significant issue, not least because the approach in the current Bill will legalise what appears from the Senate Committee's report to be a current practice of AFP to use ordinary search warrants to access 'stored communications' between private individuals

even if those communications have not been read. As noted above, the Attorney-General's Department considers that current law does not authorise access in such a way.

In addition, Parliament might note that in the February Bill, the Government tried to address concerns about the invasion of privacy raised in relation to the 2002 Bill. But with the current Bill, the Government is proposing an even broader exclusion – albeit temporary – from the protections of the Telecommunications (Interception) Act for 'stored communications' than that criticised in the 2002 Bill. Access to such communications before they have been read by the intended recipient will be allowed under the ordinary search warrant process, which has been designed to obtain physical evidence not gain access to personal communications. Consequently there is no specific requirement in the ordinary search warrant process to consider privacy issues.

As Bills Digest No 111 of 2003-04 noted:

> Access to private communications…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. The Act…contains strict protocols on use and handling of information collected by means of interception warrants…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.[19]

Parliament will need to consider whether exclusion of 'stored communications' from the regime in the Telecommunications (Interception) Act for a 12 month period as proposed in the current Bill is justified by the operational and practical reasons cited by the Attorney-General.

Endnotes

1 http://www.aph.gov.au/library/pubs/bd/2003-04/04bd111.pdf.

2 http://www.aph.gov.au/senate/committee/legcon_ctte/tel_intercept04/report/report.pdf.

3 Senate Legal and Constitutional Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2004*, Canberra 2004, p. 16.

4 ibid.

5 ibid., p. 17.

6 Ibid., p. 27.

7 Philip Ruddock (Attorney-General), 'Second reading speech: Telecommunications (Interception) Amendment (Stored Communications) Bill 2004', House of Representatives, *Debates*, 27 May 2004, p. 29130.

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

9 Ruddock, 'Second reading speech: Telecommunications (Interception) Amendment Bill 2004, *Debates*, 19 February 2004, p. 25230.

10 'Explanatory memorandum: Telecommunications (Interception) Amendment (Stored Communications) Bill 2004', p. 6.

11 Ruddock, Stored Communications Bill, op. cit.

12 ibid.

13 Explanatory memorandum, p. 3.

14 Subsequent sections contain exceptions to this general prohibition.

15 Explanatory memorandum, p. 3.

16 ibid.

17 http://www.aph.gov.au/library/pubs/bd/2003-04/04bd147.htm.

18 Jennifer Norberry, 'Surveillance Devices Bill 2004', *Bills Digest*, no. 147, 2003-04 Parliamentary Library, Canberra,.

19 Peter Prince, 'Telecommunications (Interception) Amendment Bill 2004, *Bills Digest* no. 111, 2003-04 Parliamentary Library, Canberra,.