The Senate

Legal and Constitutional Legislation Committee

Provisions of the Telecommunications (Interception) Amendment Bill 2004

March 2004

ISBN 0 642 71381 2

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

MEMBERS OF THE LEGISLATION COMMITTEE

Members

Senator Marise Payne, **Chair**, LP, NSW
Senator the Hon. Nick Bolkus, **Deputy Chair**, ALP, SA
Senator Brian Greig, AD, WA*
Senator Joseph Ludwig, ALP, QLD+
Senator Brett Mason, LP, QLD
Senator Nigel Scullion, CLP, NT

Substitute Member

* Senator Aden Ridgeway, AD, NSW to replace Senator Brian Greig for matters relating to the Indigenous Affairs portfolio

\+ Senator Kerry O'Brien, ALP, TAS to replace Senator Joseph Ludwig for matters relating to the Indigenous Affairs portfolio

Participating Members

Senator the Hon. Eric Abetz, LP, TAS
Senator Mark Bishop, ALP, WA
Senator George Brandis, LP, QLD
Senator Bob Brown, AG, TAS
Senator Kim Carr, ALP, VIC
Senator Grant Chapman, LP, SA
Senator Alan Eggleston, LP, WA
Senator Christopher Evans, ALP, WA
Senator the Hon. John Faulkner, ALP, NSW
Senator Alan Ferguson, LP, SA
Senator Jeannie Ferris, LP, SA
Senator Brian Harradine, IND, TAS
Senator Leonard Harris, PHON, QLD
Senator Gary Humphries, LP, ACT
Senator Linda Kirk, ALP, SA
Senator Susan Knowles, LP, WA
Senator Meg Lees, APA, SA
Senator Ross Lightfoot, LP, WA
Senator Sue Mackay, ALP, TAS
Senator Julian McGauran, NPA, VIC
Senator Jan McLucas, ALP, QLD
Senator Shayne Murphy, IND, TAS
Senator Kerry Nettle, AG, NSW
Senator Robert Ray, ALP, VIC
Senator the Hon. Nick Sherry, ALP, TAS
Senator Ursula Stephens, ALP, NSW
Senator Natasha Stott Despoja, AD, SA
Senator Tsebin Tchen, LP, VIC
Senator John Tierney, LP, NSW
Senator John Watson, LP, TAS

Senator Andrew Bartlett, AD, QLD for matters relating to the Immigration and Multicultural Affairs portfolio.

Secretariat

Ms Louise Gell	Secretary
Mr Phillip Bailey	Principal Research Officer
Ms Marina Seminara	Executive Assistant

Suite S1.61
Parliament House

Telephone: (02) 6277 3560
Fax: (02) 6277 5794
E-mail: legcon.sen@aph.gov.au

TABLE OF CONTENTS

RECOMMENDATIONS

Recommendation 1

The Committee recommends that Parliamentary consideration of proposed subsections 6(1) 6(5), 6(6) and 6(7) 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 Bill.

Recommendation 2

The Committee supports the remaining provisions of the Bill, and the Committee recommends that the remainder of the Bill proceed.

ABBREVIATIONS

2002 Bill	Telecommunications Interception Legislation Amendment Bill 2002
AFP	Australian Federal Police
CDPP	Commonwealth Director of Public Prosecutions
EFA	Electronic Frontiers Australia Inc.
ISP	Internet Service Provider
LEA	law enforcement agency
MMS	Multi-media Messaging Service
SMS	Short Messaging Service
the Act	*Telecommunications (Interception) Act 1979*
TI regime	Telecommunications Interception Regime
TI warrant	Telecommunications Interception Warrant
VOIP	Voice Over Internet Protocol

CHAPTER 1

INTRODUCTION

1.1 On 3 March 2004, the Senate referred the Telecommunications (Interception) Amendment Bill 2004 to the Legal and Constitutional Legislation Committee for inquiry and report by 30 March 2004.

Key provisions of the Bill

1.2 The Bill amends the Act to:

- extend the availability of telecommunications warrants to additional serious offences;
- extend the protections of the Act in relation to text based communications;
- facilitate the recording of calls to publicly listed ASIO numbers; and
- clarify the application of the Act to delayed access message services (eg email and SMS).

Conduct of the inquiry

1.3 The Committee wrote to over 50 individuals and organisations inviting submissions by 12 March 2004. Details of the inquiry, the Bill and associated documents were also placed on the Committee's website.

1.4 The Committee received 15 submissions, including six supplementary submissions, and these are listed at Appendix 1. Submissions were placed on the Committee's website for ease of access by the public.

1.5 The Committee held one public hearing in Canberra on 22 March 2004. 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.

Acknowledgment

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

Notes on references

1.7 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

BACKGROUND TO THE BILL

2.1 This chapter briefly outlines the background and the main provisions of the Bill in relation to:

- amending Class 1 offences to include terrorist activities;
- extending the scope of cybercrimes covered by the Act;
- extending the definition of 'interception' to include reading or viewing;
- communications to publicly listed ASIO numbers;
- delayed access message services – access to stored communications
- removing the requirement for ASIO to notify carriers of interception warrant where carrier not required to act; and
- allowing a certifying officer of an agency to determine when a warrant is no longer required.

Background

2.2 Amongst other things, the Bill seeks to update the *Telecommunications (Interception) Act 1979*, to ensure that electronic communications such as email and SMS are covered in an analogous manner to telephone calls under the Act.

2.3 The Committee previously inquired into the Telecommunications Interception Legislation Amendment Bill 2002 (the 2002 Bill). Evidence to that inquiry suggested that the 2002 Bill was not sufficiently clear as to whether stored communications, such as emails and SMS could be accessed by law enforcement agencies (LEAs) under a search warrant on the premises of an internet service provider (ISP) or whether a telecommunications interception warrant (TI warrant) was required. The Committee recommended in relation to the 2002 Bill:

> … that the Attorney-General review the current law on access to stored communications of delayed message services with a view to amending the Telecommunications Interception Legislation Amendment Bill 2002 so that the accessing of such data requires a telecommunication interception warrant.[1]

---

1 Senate Legal and Constitutional Legislation Committee, *Telecommunications Interception Legislation Amendment Bill 2002*, May 2002. p. 64.

2.4 The relevant provisions of the 2002 Bill did not proceed.

2.5 The Attorney-General's Department states in its submission to the inquiry that the Bill does not extend broader powers in relation to access to email and SMS:

> The amendments in fact more clearly protect text and image based communications, such as email and SMS, and clarify how the Act applies to those telecommunications where there is a delay between sending and final receipt of a message.[2]

2.6 The Attorney-General's Department also states in its submission that the concerns raised in the Committee's 2002 inquiry have been addressed, and that under this Bill emails that are stored at an ISP, and have not been read by the recipient, will not be accessible by LEAs without a TI warrant.[3] This is arguably not so clear, as proposed subsections 6(4) and 6(5) of the 2002 Bill appear (in practical effect, not verbatim) to have been reproduced in proposed subsection 6(7) of the current Bill.

Amending Class 1 offences to include terrorist activities

2.7 Item 1 of the Bill amends the definition of Class 1 offences in the Act to include offences against the following parts of the *Criminal Code*: Division 72 (offences relating to terrorist activities using explosive or lethal devices), Division 101 (terrorism offences, including engaging in a terrorist act, providing or receiving training connected with terrorist acts), Division 102 (offences in relation to terrorist organisations, including directing the activities of a terrorist organisation) and Division 103 (offence of providing or collecting funds to facilitate or engage in a terrorist act).

2.8 The effect of the amendment is to allow law enforcement agencies to apply for a warrant authorising the interception of telecommunications where information that may be obtained would be likely to assist in the investigation of offences set out in those Divisions. This Item would be effected by the insertion of paragraph 5(1)(cb) in relation to the definition of a Class 1 offence, which would supplement the existing 5(1)(ca) which allows a telecommunications interception warrant to be sought in connection with the investigation of 'an offence constituted by conduct involving an act or acts of terrorism'.

---

2 Attorney-General's Department, *Submission 6*, p.3.

3 Attorney-General's Department, *Submission 6*, p.7.

Extending the scope of cybercrimes covered by the Act

2.9 Item 4 extends the range of cybercrime offences that may be the subject of a telecommunications interception warrant under Part 10.7 of the *Criminal Code* to include a range of State and Territory cybercrime offences.[4]

Extending the definition of 'interception' to include reading or viewing

2.10 Item 5 amends the definition of interception in subsection 6(1) to include reading or viewing a communication in the definition of interception. This enables the definition of interception to include communications that are in a written form such as email and SMS etc.

Communications to publicly-listed ASIO numbers

2.11 Item 10 inserts two new subsections into section 6 of the Act to allow ASIO to listen, record, read or view any communication to a publicly listed ASIO number. Whilst this is already done by ASIO, this provision would remove the requirement that ASIO notify callers that their call is being recorded.

Delayed access message services – access to stored communications

2.12 Item 10 also amends section 6 of the Act to clarify where a stored communication has ceased passing over a telecommunications system (and as a result a law enforcement agency does not require a TI warrant to access it).

2.13 The amendment does this by adding three new subsections to section 6 of the Act,[5] which in order, define 'delayed access message service', 'stored communication', and when a stored communication is not taken to be passing over a telecommunication system.

2.14 The definition of 'delayed access message service' is a means by which a communication can be intended for a person without them being in direct contact with the sender, and can be subsequently accessed (by the receiver or other persons), but specifically excludes Voice Over Internet protocol (VOIP). VOIP is a method by which voice (ie a two way telephone conversation) can be made through packet switching technology (ie the way data moves over the internet). VOIP is becoming an

---

4 This covers a series of existing State and Territory cybercrime offences, and for those States and Territories that do not currently have such offences, any corresponding offences that may be enacted in the future. The extra offences to be included are: section 308C, 308D, 308E, 308F, 308G, 308H or 308I of the Crimes Act 1900 of New South Wales; section 247B, 247C, 247D, 247E, 247F, 247G or 247H of the Crimes Act 1958 of Victoria; a provision of a law of a State (other than New South Wales or Victoria) that corresponds to a provision covered by paragraph (a), (b) or (c); a provision of a law of a Territory that corresponds to a provision covered by paragraph (a), (b) or (c); section 440A of The Criminal Code of Western Australia.

5 Proposed subsection 6(5), 6(6),6(7).

increasingly popular method of making telephone calls (due to the drastically reduced cost), and presumably by excluding it, ensures that where interceptions of such communications are intended, a telecommunications interception warrant *is* required.

2.15 For practical purposes the definition of 'delayed access message service' includes SMS, MMS, email and voice mail on a mobile phone (but excludes VOIP).

2.16 The definition of 'stored communication' is a communication that has been submitted using a delayed access message service, and is stored on equipment.

2.17 Proposed subsection 6(7) operates by setting out the circumstances when stored communications are taken *not* to be passing over a telecommunications system (and hence when such access does *not* require a telecommunications interception warrant). These circumstances are as follows:

- when it is accessed by or with the authority of the intended recipient;[6]
- when it is accessed by another person after the receiver has accessed it (or with their consent), so long as it is accessed by the other person without using a telecommunications service or other form of remote access, unless it is merely for the purposes of, or an incidental result of turning on obtaining power required to run the equipment (or any other action prescribed by regulations);[7] or
- when it is accessed by another person using any or all of the equipment which the intended recipient could have used to access the stored communication (or any or all of that equipment in combination with other equipment), so long as it is accessed by the other person without using a telecommunications service or any other form of remote access, unless the use of that service is merely for the purpose of or an incidental result of, turning on or obtaining power required to operate the equipment (or any other action prescribed by regulations).[8]

2.18 In relation to the proviso that a telecommunications service or other remote access service not be used, unless it is merely for the purpose of, or an incidental result of, turning on or obtaining power required to operate the equipment, the Explanatory Memorandum states that when a mobile phone is turned on, it automatically communicates with the telecommunications service in order to locate the nearest base station.[9] Similarly, fixed line phones (which have the capacity to operate as a 'delayed access message service') are often powered through the telecommunications line.[10]

---

6 Proposed s 6(7)(a)

7 Proposed s 6(7)(b)

8 Proposed s 6(7)(c)

9 Telecommunications (Interception) Amendment Bill 2004, *Explanatory Memorandum*, p.7.

10 Telecommunications (Interception) Amendment Bill 2004, *Explanatory Memorandum*, p.7.

2.19 The effect of these provisions in relation to ISP email (ie email involving an internet service provider account), would mean that a law enforcement agency would be able to read emails that have been accessed and stored by the recipient, as well as obtain a copy from the ISP (because neither of these has entailed using a telecommunications service or other remote access), but could not use the internet to access the recipients account directly (as this would be using a telecommunications system).

2.20 In the case of SMS or MMS, because messages are generally delivered and stored directly to the recipient's handset, a law enforcement agency would not require a telecommunications interception warrant to view or read such messages if they are only doing so by powering up the recipient's handset, or using other equipment to read the recipient's sim card. Again, this is because such action does not require access or use of a telecommunications network, other than for the incidental act of powering up the handset.[11]

2.21 In the case of voice mail for mobile telephones, a law enforcement agency can access the stored messages on the handset once the recipient has accessed the message (or could seek to obtain a copy of the message from the service provider) but would require a telecommunications interception warrant in order to access the messages by use of the telecommunications system.

ASIO no longer required to notify telecommunication carriers of interception warrant where carriers not required to act

2.22 The effect of proposed paragraph 15(1A)(ba) is that where ASIO is granted an interception warrant, it would no longer be required to advise a telecommunications carrier of the interception activity if no action by the telecommunications carrier is required. Conversely, if the interception does require action on the part of the carrier or its employees, such notification will be required (proposed paragraph 15(4)(ba)).

Certifying officer of an agency able to determine warrant no longer required

2.23 Items 17 and 18 of the Bill will amend paragraph 60(5)(b) to extend the range of persons within an agency who may determine that an interception is no longer required, to include a certifying officer of an agency. The purpose of this is to expedite the cessation of an interception where it is no longer required.[12]

---

11 Telecommunications (Interception) Amendment Bill 2004, *Explanatory Memorandum*, p.7.

12 Telecommunications (Interception) Amendment Bill 2004, *Explanatory Memorandum*, p.10.

CHAPTER 3

DELAYED ACCESS MESSAGE SERVICES

3.1 This chapter discusses the significant concerns raised in submissions and evidence in relation to the provisions of the Bill which seek to clarify how the telecommunications interception regime applies to the access of stored communications of delayed access message services (such as emails, SMS, MMS, and voicemail). The relevant provisions are those that extend the definition of 'interception' to include reading or viewing, and the exceptions to when a telecommunications interception warrant is required in relation to accessing a stored communication (these amendments include proposed subsection 6(1), 6(5), 6(6), and 6(7) in Items 5 and 10 of the Bill).

Key issues

3.2 The Australian Federal Police (AFP) did not support proposed subsections 6(1), 6(5), 6(6) and 6(7) of the Bill, and argued that as drafted they could impair the AFP's capacity to protect its information systems and conduct effective investigations.[1]

3.3 Other submissions that commented on these aspects of the Bill supported the intention of the Bill, but raised concerns over unintended consequences and suggested various amendments to clarify the operation of the Bill.

3.4 The following issues were raised and are discussed in turn below:

- e security and corporate governance – recording;
- e security and corporate governance – reading or viewing;
- search warrants – retrieval of stored communications;
- exceptions to the need for a TI warrant;
- requirement that communication has been accessed by recipient;
- retrieval of stored communications held remotely;
- search warrants at ISPs;
- meaning of ‘when’ in proposed paragraph 6(7)(a);
- exclusion of Voice Over Internet Protocol from ‘delayed access message services’;

---

1 Australian Federal Police, *Submission 7*, p.4.

- application of the Bill to 'voice and text' and 'chat sessions';
- access not limited to law enforcement agencies; and
- access by or with the intended recipient's authority.

E security and corporate governance - recording

3.5 The AFP raised concerns in relation to the ability of organisations seeking to filter incoming and outgoing emails by copying and viewing them. The AFP noted that in its organisation, emails are copied and scanned by email filtering software. If an anomaly is detected the email is 'quarantined' and the employee is notified. The employee can ask for the release of quarantined emails: otherwise the email is deleted after 7 days.[2]

3.6 The AFP noted that where a private entity or government agency seeks to protect incoming and outgoing emails, and copies emails at the gateway or firewall (which is considered 'best practice') this may be considered a 'recording' and therefore constitute an 'interception' under the Bill.[3]

3.7 This is similar to a concern put forward by Electronic Frontiers Australia Inc. (EFA) that where ISPs copy or backup emails for the purposes of disaster recovery, they may technically be considered to be making a recording, and hence require a TI warrant in order to make such copies.[4]

3.8 EFA also noted that where such copies or back ups have been made, where a law enforcement agency seeks to use such material gained lawfully, it may not be admissible as the original copy was made in an unlawful manner. EFA also pointed out this could have consequences for the ISP or carrier, as they may be subject to a civil remedy under section 107A of the Act.[5]

3.9 EFA argued that the Bill should be amended so that the act of ISPs making backups does not involve a stored communication passing over the telecommunications system.[6]

3.10 In response the Attorney-General's Department stated that it considered such amendments unnecessary as the Act is directed at protecting the privacy of users of the Australian telecommunications system, and automated backup for the purpose of

---

2 Australian Federal Police, *Submission 7*, p.7.

3 ibid.

4 Electronic Frontiers Australia Inc., *Submission 1*, p.8.

5 ibid.

6 Electronic Frontiers Australia Inc., *Submission 1*, p.14.

business continuity does not impinge upon the Act's object of protecting the privacy of communications.[7]

E Security and corporate governance – reading or viewing

3.11 The AFP argued that not only might its copying of emails but also its reading or viewing suspect or quarantined emails fall within the TI regime of the Bill. The AFP stated that this might compromise its ability to conduct internal integrity checking.[8]

3.12 On this issue, it is important to make a distinction over two types of 'reading'. There is the reading that may occur automatically or digitally, where a virus or image filtering software program 'reads' incoming emails for suspect content. On the other hand, the AFP expressed concern that their integrity systems often involve human reading, as those emails that are detected automatically as being suspect are then viewed by a person.[9]

3.13 In response the Attorney-General's Department argued that automatic or computer reading of a communication does not fall within the meaning of 'reading' as it appears in the Bill. The Department argued that this is currently the case, and would not change under the Bill.[10] The Department also noted that the Solicitor-General had addressed the question in an opinion, and had stated that under the proposed amendments, reading and viewing are limited to human reading or viewing, or at least to reading or viewing in a manner that would result in the sense and meaning of the message being apprehended and understood.[11]

3.14 However in relation to human reading or viewing of such emails (as opposed to computerised filtering or reading), the Attorney-General's Department confirmed in the hearing that the current integrity systems used by the AFP, where a person reads suspect emails would not be permitted under the Bill (without a TI warrant).[12]

3.15 In the hearing, the Attorney-General's Department was asked if they had consulted with the AFP over this issue. A representative indicated that the issue had been raised in January 2004 when consulting over the Bill. The Department reiterated

---

7 Attorney-General's Department, *Submission 6A*, p.2.

8 Australian Federal Police, *Submission 7*, p.8.

9 ibid.

10 Attorney-General's Department, *Submission 6A*, p.4.

11 Attorney-General's Department, *Submission 6B*, p.4.

12 *Committee Hansard*, 22 March 2004, p.20.

that electronic filtering would still be available under the Bill, and that in their own integrity system filtering was limited to such electronic form.[13]

3.16 Adding to the confusion, are questions as to whether the Bill would in fact apply to activities on a private network. This could mean that once an email moves from the public telecommunications network through a firewall and onto the private network of a company or organisation, what that company or organisation does between the passing of the firewall to receipt by the individual may in fact not be regulated by the Bill. At the hearing EFA explained:

> Our interpretation of the existing legislation and the proposed bill suggests to us that the situation would not be quite as dire as the Australian Federal Police appear to think it would be. We think that there may be an issue in the definition of 'passing over the telecommunications system'. Our understanding is that that telecommunications system may well cease at the boundary between an Internet service provider's system and a private corporation's system.
>
> This matter has been raised before in front of this committee in relation to the Cybercrime Bill 2001. I understand that the Attorney-General's Department advised the committee that a private network probably could not be regulated by the Commonwealth because of the provisions of section 51 of the Constitution. We think that there is a question here as to whether, in the same way that the Cybercrime Act was said not to apply to computers and networks in a private business, the Telecommunications (Interception) Act would in fact apply to email messages once they had been received on the business's equipment. Unlike a telephone call, once an email message has passed across into the private business network, the communication is no longer on the public network the way a telephone call is.[14]

3.17 At the hearing the AFP confirmed that there is uncertainty regarding this matter, and argued that consideration should be given to the United Kingdom regulatory regime and making an exemption in the Bill, such that those operating private networks are permitted to do certain acts in order to protect their systems and business operations:

> ... the UK regulations have actually addressed those issues and recognised that the owners of private communications networks should be allowed to do certain acts, such as open and view, in the course of that business to protect their own systems and business operations.[15]

---

13 *Committee Hansard*, 22 March 2004, p.20.

14 Ms Irene Graham, *Committee Hansard*, 22 March 2004, p.2.

15 *Committee Hansard*, 22 March 2004, p.13.

3.18 In a supplementary submission to the Committee the Attorney-General's Department addressed this issue, arguing that in the Department's opinion, the telecommunications network extends to all equipment within Australia connecting a user to the public switched telephone network, up to and including a user's personal equipment. The Department stated that it had received independent legal advice supporting this view.[16]

3.19 The Department provided the following clarification in relation to EFA's comments on what the Department said about private networks in the 2001 Cybercrime Bill inquiry:

> The Act would only not apply in circumstances where a system for carrying communications was purely private, that is, where the relevant system had no connectivity to any public telecommunications services. The comments of the Attorney-General's Department to the Committee in its inquiry into the provisions of the Cybercrime Bill 2001 were made in that context….. The Department did not indicate, and does not support the view, that the telecommunications system ceases at the boundary between a service provider's system and the customer's equipment.[17]

Search warrants – retrieval of stored communications

3.20 The AFP expressed concern that where an officer is executing a search warrant, and discovers that there is an email message that is available for retrieval (that is, it has not been accessed), he or she would be required to obtain a TI warrant to gather potentially important evidentiary material. The AFP argued that this would lead to a delay and could allow a suspect to delete the message. [18]

Exceptions to the need for a TI warrant

3.21 The AFP criticised the exceptions to the requirement to obtain a TI warrant specified in proposed subsections 6(5), 6(6), and 6(7). The AFP argued that because these exceptions demand that the access not involve use of the telecommunications or remote access service, access to web-based email will always require a TI warrant, even where the email in question has been accessed by the recipient. [19]

3.22 The AFP also pointed out that as some agencies do not have access to TI warrants (such as ASIC, Australian Customs Service and the Queensland Police

---

16 Attorney-General's Department, *Submission 6D*, p.2.

17 ibid.

18 Australian Federal Police, *Submission 7*, p.8.

19 Australian Federal Police, *Submission 7*, p.10.

Service) they will be severely restricted where suspects make use of such email services. [20]

3.23 Whilst the AFP argued that the Bill would require it to obtain a TI warrant whenever dealing with web-based email, the Victorian Privacy Commissioner expressed concern that the Bill was not clear enough in ensuring that emails stored in transit are 'passing over a telecommunications system' and hence protected by the TI regime. The Victorian Privacy Commissioner proposed that the Bill should express what is to be protected, rather than simply stating in which circumstances a communication is not passing over a telecommunications system.[21]

3.24 The Attorney-General's Department stated in its submission that communications that have not been accessed, including those that remain in transit at the ISP, will continue to be protected by the TI regime, and that under the Bill access would require a TI warrant.[22]

3.25 The Department noted that under the Bill unread emails stored at the ISP would require a TI warrant in order to be obtained. This was because any access not involving a telecommunications line or remote connectivity would necessarily be at the ISP's premises for storing the communication, and the recipient could not ordinarily have been able to physically enter the ISP to extract the email.[23]

Requirement that communication has been accessed by recipient

3.26 The AFP explained that the requirement in proposed subparagraph 6(7)(b), that a message has been accessed by the recipient, will also be problematic in regards to email, as it may be impossible to ascertain whether a message has been accessed.[24]

3.27 At the hearing the Committee asked the Attorney-General's Department what would be required where law enforcement agencies seeking to obtain access to emails from an ISP were unsure of whether they had been read.[25] The Department stated that if in doubt, the Department would suggest the law enforcement agency should obtain a TI warrant.[26]

---

20 Australian Federal Police, *Submission 7*, p.10.

21 Victorian Privacy Commissioner, *Submission 5*, p.4.

22 Attorney-General's Department, *Submission 6*, p.5.

23 ibid.

24 Australian Federal Police, *Submission 7*, p.10.

25 *Committee Hansard*, 22 March 2004, p.18.

26 ibid.

3.28 Due to the AFP's opposition to these provisions of the Bill, the Committee asked the AFP to whether they were satisfied with the degree to which they had been consulted over the Bill. The AFP commented:

> There has been consultation on a range of matters. I understand that in this particular circumstance time precluded there being the level of consultation that we might have liked, given those considerations.[27]

Retrieval of stored communications held remotely

3.29 According to the AFP, the Bill's requirement that a TI warrant be obtained in order to remotely access material is inconsistent with the intentions of section 3L of the *Crimes Act 1914* (amended by the Cybercrime Bill 2001). [28]

3.30 The AFP pointed out that subsection 3L(1) of the *Crimes Act 1914* allows investigating officers acting under authority of a search warrant the power to operate equipment at the premises to access data held remotely and that the Bill will operate in opposition to this. [29] The AFP pointed out that the Committee had inquired into the provisions of the Cybercrime Bill 2001 and made no adverse recommendations in respect of remote access powers. [30]

3.31 In its supplementary submission prior to the hearing, the Attorney-General's Department argued that this interpretation of section 3L of the *Crimes Act 1914* was incorrect, and that the provisions of that Act do not override the specific protections conferred upon communication by the interception legislation.[31]

3.32 This matter was discussed further at the hearing. The AFP confirmed that advice from the Commonwealth Director of Public Prosecutions (CDPP) had been that where AFP officers enter premises under a search warrant and discover a computer with both read and unread emails, section 3L of the *Crimes Act 1914* enables them to read both types of emails.[32]

3.33 At the hearing the Attorney-General's Department noted that there was some lack of clarity:

---

27 *Committee Hansard*, 22 March 2004, p.10.

28 Australian Federal Police, *Submission 7*, p.11.

29 Australian Federal Police, *Submission 7*, p.11.

30 Australian Federal Police, *Submission 7*, p.11.

31 Attorney-General's Department, *Submission 6A*, p.4.

32 *Committee Hansard*, 22 March 2004, p.11.

> The reason we do not have clarity in the one area that has been discussed, namely 3L, is that we—the department administering the legislation—take the view that the current legislation is clear on this issue but the DPP has taken a different view. In light of that, we have asked the AFP to provide us with all the material that they have that has led the DPP to form this conclusion, and we have sought the opinion of the Solicitor-General on this. That opinion has not yet arrived.[33]

3.34 Following the hearing, the Attorney-General's Department noted that parts of the Solicitor-General's opinion had been provided to it and outlined that advice in its second supplementary submission:

> The Solicitor-General notes in his Opinion that those amendments that seek to specify a range of circumstances in which delayed access message service communications are taken to have ceased their passage over the telecommunications system clarify the current state of the law. Those amendments are consistent with the current operation of the prohibition against interception, and do not change the means by which communications may be accessed by law enforcement agencies. The current operation of the law would, as the Department indicated in its evidence, 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.[34]

3.35 The Attorney-General's Department position is clearly that section 3L of the *Crimes Act 1914* does not permit the AFP to retrieve unread emails and voice messages using handsets and computers that they encounter when executing search warrants.

3.36 However, the AFP's supplementary submission (responding to the Attorney-General's Department's first supplementary submission) stated:

> The AFP notes that section 3L of the *Crimes Act* is a later provision that was introduced without reference to limitations under the TI Act to this kind of information. The intention of 3L was clearly to allow access to stored communications held remotely under the auspices and accountabilities of the search warrant regime.
>
> The Department's interpretation of the specific protections of the TI Act relies on their interpretation, which is based on the broad underlying policy of the Act. The AFP's position is based on CDPP advice which appears to rely on the specific provisions of the *Crimes Act 1914.*

---

33 *Committee Hansard*, 22 March 2004, p.15.

34 Attorney-General's Department, *Submission 6B*, p.3.

> The AFP considers that considerable confusion may have arisen as a result of the difference between the legal and policy views held by the CDPP and the Department respectively.[35]

3.37 The AFP argued that if Item 10 of the Bill were to proceed, it should be amended so that there is an exemption for law enforcement agencies seeking to make use of section 3L of the *Crimes Act 1914*:

> In relation to overcoming the severe operational difficulties that the proposed amendment in item 10 of the Bill will impose, the AFP remains of the view that where access to a stored communication held remotely is done under the lawful authority of another Act, there should be an express exemption under the TI Act for this purpose. This approach would enable the AFP to secure important evidence in a timely manner, and in a best case scenario, to act quickly in the interests of preventing, for example, a terrorist incident.[36]

Search warrants at ISPs

3.38 The AFP argued that the difficulties that law enforcement agencies may face in executing search warrants on emails that are stored at an ISP are inconsistent with the powers they have in regard to accessing traditional mail delivered at a post office box. They argued that mail at post office boxes and email at ISPs are analogous, and law enforcement agencies should have equivalent powers under a search warrant.[37]

3.39 This argument runs contrary to the main policy behind the Bill, namely, that emails are not like mail, but rather, are a form of telecommunication like a phone call.

3.40 The special nature of email was emphasised by EFA at the hearing, when they were asked why emails should be treated differently to traditional mail:

> [W]ith a postal mail letter, you basically do not leave it in the post office. So the fact that you are leaving messages on an ISP server in the first place signifies another aspect of the difference between the way letter mail operates and the way telecommunications operates. With postal mail, all copies of your old letters are not left stored in the post office. In the letter environment that just does not happen, but it does with email. The whole telecommunications process is completely different from letter mail. We think communications through the various telecommunications need different levels of protection from that for standard letters. That has always

---

35 Australian Federal Police, *Submission 7A*, p.2.

36 Australian Federal Police, *Submission 7A*, pp.2-3.

37 Australian Federal Police, *Submission 7*, p.12.

> been the case to date. We think of email as a continuation of the telephone call environment.[38]

Meaning of 'when' in proposed paragraph 6(7)(a)

3.41 EFA argued in its submission that the wording of proposed subparagraph 6(7)(a) in the Bill is unclear, and could give rise to two different interpretations:

> 6(7) For the purposes of this section, a stored communication that is intended for a person (the intended recipient) is taken not to be passing over a telecommunications system:
>
> > (a) when it is accessed by or with the authority of the intended recipient…

3.42 EFA suggest that this could be interpreted as meaning a stored communication is not passing over a telecommunications system at the exact time that the message is retrieved, which would mean at that moment it is not protected by the TI regime. EFA acknowledge such a narrow interpretation is unlikely given the overall intention of the Bill, but suggest that this should be clarified.[39]

3.43 This was also pointed out in the *Bills Digest* as a possible drafting error.[40]

3.44 The Attorney-General's Department argued that such an interpretation would be inconsistent with both the intention of the amendments as outlined in the Explanatory Memorandum, and the underlying objects of the Act.[41]

Exclusion of VOIP from 'delayed access message services'

3.45 The Australian Privacy Foundation noted that Voice Over Internet Protocol (VOIP) had been excluded from the definition of delayed access message services, and agreed with this, but suggested that to ensure that VOIP is covered by the TI regime that the Bill should explicitly clarify this to remove any doubt. [42]

3.46 This point was also made by the Victorian Privacy Commissioner.[43]

---

38 Ms Irene Graham, *Committee Hansard*, 22 March 2004, p.6.

39 Electronic Frontiers Australia Inc, *Submission 1*, p.8.

40 *Telecommunications (Interception) Amendment Bill 2004*, Bills Digest No.111 2003-04. Department of Parliamentary Services, p.9.

41 Attorney-General's Department, *Submission 6A*, p.2.

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

43 Victorian Privacy Commissioner, *Submission 5*, p.6.

3.47 The Attorney-General's Department stated in its submission that VOIP has been excluded from the definition of 'delayed access message services' because it is to be treated like standard telephony.[44]

Application of Bill to 'voice and text' and 'chat sessions'

3.48 The Victorian Privacy Commissioner was concerned that the Bill was not sufficiently clear in regard to communications that involve both text and voice. Such communications include exchange of text in a 'chat session' as well as VOIP (that is, people typing messages instantaneously to each other while talking through packet switching technology). [45]

3.49 The Victorian Privacy Commissioner was also concerned that the Bill was silent on the issue of logs of internet 'chat sessions' which are generated automatically, but stand as a recording of the communication.[46] This is an important issue as such logs are important evidence in cases where law enforcement agencies conduct undercover chats with suspected paedophiles.

3.50 The Attorney-General's Department explained:

> 'Chat' type communications pass over the telecommunications system, and are therefore protected by the Act during their passage over that system. While offering relative immediacy of communication, such messages may be temporarily delayed during their transit between sender and recipient…. Access to chat communication will require a telecommunications interception warrant in circumstances where access is sought prior to display of the chat message on the recipient's computer. However, access after the recipient has viewed the message would not amount to interception where effected in accordance with the access mechanisms outlined in proposed subsection 6(7)(b) and (c).[47]

Access not limited to law enforcement agencies

3.51 Because the Bill specifically refers to a person being exempted from the need to obtain a TI warrant as 'another person', the Victorian Privacy Commissioner was concerned that as long as the criteria are met in proposed subsections 6(7), then a person's accessed emails could be read by anyone, not just a law enforcement agency.[48]

---

44 Attorney-General's Department, *Submission 6*, p.7.

45 Victorian Privacy Commissioner, *Submission 5*, p.6.

46 ibid

47 Attorney-General's Department, *Submission 6D*, pp.1-2.

48 Victorian Privacy Commissioner, *Submission 5*, p.7.

3.52 The Attorney-General's Department responded:

> It is not necessary to include a provision of this kind because the amendments do not allow unregulated access to communications that are no longer passing over a telecommunications system. Where a telecommunications interception warrant is not required in order to access a particular communication, because that communication has ceased its passage over the telecommunications system, the person seeking access may nevertheless only access the communication in accordance with some other form of lawful authority, such as a search warrant.[49]

Access by or with the intended recipient's authority

3.53 The Victorian Privacy Commissioner was concerned that the reference to 'authority' in proposed subsection 6(7) was not sufficiently clear, in that it could mean express authority when confronted by a law enforcement agency, but could also mean apparent authority arising out of a contract with an ISP. The Victorian Privacy Commissioner suggested that in cases of apparent authority, the recipient should be notified that their communications have been accessed (subject to certain qualifications).[50]

3.54 The Attorney-General's Department stated in response:

> It is not necessary for the amendments to include such a requirement - clear and unambiguous authority will be required in order to attract the operation of the provision. By conferring such authority the recipient will by necessary implication be aware of the communications that the authorised person may have access to.[51]

The Committee's view

3.55 In its previous inquiry the Committee was concerned that the 2002 Bill did not ensure sufficient protection for stored communications of delayed access message services (email, SMS, MMS, and voicemail) and suggested a review. Those provisions did not proceed. In light of this, the Committee was interested in ensuring that its concerns in relation to the application of the telecommunications interception regime to stored communications of delayed access message services had been addressed in relation to the current Bill.

3.56 The Committee is satisfied that in relation to access of stored communications of delayed access message services, the intent of the Bill is to clarify the current state of the law.

---

49 Attorney-General's Department, *Submission 6A*, p.3.

50 Victorian Privacy Commissioner, *Submission 5*, p.7.

51 Attorney-General's Department, *Submission 6A*, p.3.

3.57 The Committee is satisfied that the intent of the Bill is to ensure that where law enforcement agencies seek to access stored communications of delayed access message services, if the message has not been accessed, they will be required to obtain a telecommunications interception warrant (unless the recipient consents to such access, or where the un-accessed stored communication is an SMS message, as such an unread message has left the telecommunications system).

3.58 In the case of read or accessed stored communication, access would be possible with lawful access to the equipment (for example through a search warrant).

3.59 Whilst that may be the intent of the Bill, the Committee is concerned that the Bill is the subject of some confusion and may not in fact offer sufficient clarification.

3.60 The confusion that exists, is in relation to the legal status of the following practices:

1. Where a law enforcement agency seeks to access a read email at an ISP server with a search warrant;

2. Where a law enforcement agency seeks to rely on section 3L of the *Crimes Act 1914* to remotely access emails from a computer that is encountered under the auspices of a search warrant; and

3. Where a party seeks to read emails for the purposes of internal integrity measures between the point of an email passing a firewall and being received by an employee.

3.61 In the first circumstance, a law enforcement agency is currently permitted to access read emails at an ISP, where they have lawful access to the ISP under the auspices of a search warrant. Under the Bill, it is intended that a law enforcement agency would still be permitted to do this (but not permitted to access any messages that have not been read without a TI warrant). However, the AFP explained in its submission and evidence that it can be impossible to determine whether a read email has in fact been read. This was confirmed by the Attorney-General's Department, who, when confronted with what a law enforcement agency would be expected to do in such a situation if the Bill were passed, responded that if in doubt, they should obtain a TI warrant. As a result, the Committee believes that if the Bill is passed unamended, it would be possible for suspects to ensure that a law enforcement agency seeking to access email communication would always be required to obtain a telecommunications interception warrant.

3.62 In relation to the second practice, the Committee heard evidence from the AFP that due to the opinion of the Commonwealth Director of Public Prosecutions, it is of the opinion that section 3L of the *Crimes Act 1914* permits it to remotely access both read and unread emails from a computer that it encounters when acting under the auspices of a search warrant. The Bill would require that such activity would require a TI warrant. The Attorney-General's Department disagreed with the evidence of the

AFP, and referred to an opinion of the Solicitor-General which states that such acts are not currently permitted under section 3L of the *Crimes Act 1914*.

3.63 The third practice occurs where an organisation seeks to read emails between the point of the firewall and receipt by an employee for the purposes of internal security or integrity measures. The Committee heard from the AFP that such activities are currently performed, but under the Bill, this would be prohibited (without a TI warrant). The Attorney-General's Department confirmed that this is correct, and that under the Bill the AFP would no longer be permitted to do this.

3.64 The Committee believes that both the powers and protections that the telecommunications interception regime provides are matters of a very serious nature.

3.65 The operation of the Act requires certainty, both to ensure that law enforcement agencies are able to determine their powers and responsibilities and to ensure that individual privacy is protected. The Bill does not provide this certainty, and as a result the Committee is unable to recommend that the Bill proceed.

3.66 The Committee is most concerned by the disagreement between the Attorney-General's Department and the AFP as to the state of the law currently in relation to the accessing of stored communications of delayed access message services, and how it will change under the Bill. As a result, the Committee recommends that Parliamentary consideration of proposed subsections 6(1), 6(5),6(6) and 6(7) be deferred until this disagreement is resolved and Parliament informed as to the outcome.

CHAPTER 4

OTHER ISSUES

4.1 This chapter discusses issues raised in submissions and evidence in relation to other aspects of the Bill.

Issues relating to other aspects of the Bill

4.2 Other aspects of the Bill which are discussed in this chapter include:

- the extension of TI warrants to cybercrime offences;
- interception of calls made to publicly listed ASIO numbers; and
- removal of requirement for ASIO to notify carrier of interception.

Extension of TI warrants to cybercrime offences

4.3 The Committee heard views expressing both support and opposition to the list of offences to be added to the TI regime by proposed subsection 5D(5).

4.4 The AFP supported this part of the Bill.[1]

4.5 The Committee received a submission from the Tasmanian Police which recommended that the list of crimes to be included be amended to include sections 257A, 257B, 257C, 257D, 257E, 257F of the *Criminal Code Act 1924* (Tas).[2]

4.6 EFA objected to this part of the Bill, arguing that although these crimes are referred to as "cybercrimes" they are in fact computer crimes, and can be committed without using a telecommunications system.[3]

4.7 Both EFA and the Australian Privacy Foundation noted that the effect of these amendments is that TI warrants would be able to be issued for computer offences involving penalties of less than 7 years imprisonment, but this would not be the case for firearms offences (which are arguably more serious offences).[4]

---

1 Australian Federal Police, *Submission 7*, p.3.

2 Tasmania Police, *Submission 9*, p.1.

3 Electronic Frontiers Australia Inc., *Submission 1*, p.15.

4 Electronic Frontiers Australia Inc., *Submission 1*, p.15.; Australian Privacy Foundation, *Submission 2*, p.1.

4.8 EFA also noted that under some of the State offences that are listed in the proposed provision, the crime can be committed without access to a telecommunications system and can be committed even where it is impossible to commit a serious computer offence.[5]

4.9 EFA suggested that the Bill should be amended to limit the availability of interception warrants to computer offences in the following circumstances:

- offences that carry a maximum penalty of 7 or more years imprisonment and where it is possible to commit the act that is the subject of the offence; and

- in the case of offences carrying a lesser penalty, investigation only of instances of the offence where a telecommunications system is used to commit the actual offence and only in instances where it is possible to commit the serious criminal offence.[6]

4.10 The Attorney-General's Department explained that the crimes being added were serious crimes that could involve serious costs to business, and emphasised that the most effective evidence for such types of crimes will often be obtained through telecommunications interception:

> Most of the existing warrantable offences in Part 10.7 of the Code and most of the equivalent State and territory offences carry maximum penalties in the range of one to 10 years imprisonment. The inclusion of these offences as warrantable offences for the purposes of the Act reflects the seriousness of the consequences of cybercrime and the fact that the best evidence for use in prosecuting these offences may be obtained by way of telecommunications interception.[7]

The Committee's view

4.11 The Committee is satisfied that the crimes that the amendments would add to the TI regime are sufficiently serious to warrant such inclusion. In relation to cybercrime offences, the Committee notes the EFA's concerns that such crimes are not inherently related to telecommunications system, but the Committee accepts the Department's point that the most effective evidence of such crimes will often be obtainable through a telecommunications interception.

4.12 The Committee is satisfied that the inclusion of such crimes is an acceptable balance between protecting the privacy of individuals and ensuring law enforcement agencies are able to effectively collect evidence of serious crimes.

---

5 Electronic Frontiers Australia Inc., *Submission 1*, p.15,16.

6 Electronic Frontiers Australia Inc., *Submission 1*, p.16.

7 Attorney-General's Department, *Submission 6*, p.9.

4.13 The Committee notes the Tasmanian Police submission proposal to include corresponding provisions of the *Tasmanian Criminal Code Act 1924*, but notes that proposed paragraph 5D(5)(d) includes any corresponding provisions to those specified in proposed paragraph 5D(5)(a),(b) or (c). This would mean that to the degree to which the Tasmanian offences are equivalent, they will be covered by these provisions.

Interception of calls made to publicly listed ASIO numbers

4.14 The Australian Privacy Foundation and EFA opposed removing the obligation of ASIO to notify callers to publicly listed numbers that the call is being recorded.[8]

4.15 Both the Australian Privacy Foundation and EFA argued that in the absence of a legitimate need for the change, there is no reason why such a warning should not be required of ASIO.[9]

4.16 The Attorney-General's Department argued that the publicly listed numbers for ASIO are an important source of information and that this amendment is necessary as requiring a warning to be given regarding the recording of a call may deter some callers from providing information.[10]

4.17 At the hearing the Attorney-General's Department provided two arguments in support of the amendments, the first was that the time it would take to warn a caller that a call is being recorded could waste valuable time in the case of critical situations, and the Department gave the example of 000 emergency numbers which are not required to give such a warning. The second argument was that callers may be deterred from supplying information if they hear that the call is being recorded.[11]

The Committee's view

4.18 Whilst the Committee does not believe that the arguments put forward by the Department in support of this amendment constitute evidence of an urgent need for this amendment, the Committee acknowledges that such recordings are already made by 000 emergency numbers. The Committee also notes that the amendments are restricted to incoming calls only, and to calls that are made to publicly listed numbers.

---

8 Australian Privacy Foundation, *Submission 2*, p.2.; Electronic Frontiers Australia Inc., *Submission 1*, p.16.

9 Australian Privacy Foundation, *Submission 2*, p.2.; Electronic Frontiers Australia Inc., *Submission 1*, p.16.

10 Attorney-General's Department, *Submission 6*, p.11.

11 *Committee Hansard*, 22 March 2004, p.21,22.

4.19 The Committee believes that whilst the benefits of such an amendment (or at least the arguments supplied regarding such benefits) are limited, the invasion of citizens' privacy as a result of such amendments is limited.

Removal of requirement for ASIO to notify carrier of interception

4.20 The Australian Privacy Foundation expressed opposition to the Bill removing the requirement that ASIO notify a carrier of an interception, where the carrier is not required to act, arguing that this requirement acts as a check on overuse, and as carrier staff have security clearance it is unnecessary.[12]

4.21 The Attorney-General's Department addressed the issue in its submission, and argued that there may be times when it is not appropriate for ASIO to have to notify a carrier of an interception (where there is no action required by the carrier), due to security or because of an emergency.[13]

4.22 In the hearing the Committee asked what consultation had been undertaken with industry on this issue. The Attorney-General's Department confirmed that they had not consulted industry, but noted that the submission made by Optus to the inquiry had not raised any concerns with this issue.[14]

The Committee's view

4.23 The Committee notes that this amendment does not grant ASIO further powers in regards to when and how often it may undertake interceptions, it simply removes the requirement to notify a carrier of an interception warrant, where the interception can be made without any actions on the part of the carrier. The Committee acknowledges that this does mean that under the amendments, ASIO would be permitted to interact with a carrier's network or system without their knowledge. For this reason the Committee was interested in whether the Attorney-General's Department had consulted industry on the matter and was disappointed that they had not.

4.24 Notwithstanding this, the Committee notified both Telstra and Optus of the inquiry, and received a submission from Optus which supported the Bill generally, and did not comment on this issue specifically.

4.25 The Committee acknowledges that there could be matters of serious national security which might require ASIO to perform interceptions under a TI warrant without notifying the carrier.

---

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

13 Attorney-General's Department, *Submission 6*, p.10.

14 *Committee Hansard*, 22 March 2004, p.23.

The Committee's conclusions and recommendations

4.26 In regards to proposed subsections 6(1), 6(5), 6(6) and 6(7), the Committee is not satisfied that the Bill will clarify the law in relation to the access of stored communications of delayed access message services.

4.27 This is mainly due to the fact that under the Bill, law enforcement agencies may not be able to determine whether emails stored at an ISP will have been read or not, and as a result will not be able to confidently determine when a TI warrant will be required. This will have the effect that law enforcement agencies may be required to obtain a TI warrant in order to access any email at an ISP, whether it has been read or not.

4.28 The Bill will also have the effect of preventing law enforcement agencies from engaging in human review of suspect emails as they enter and leave the firewall (an act they currently legally perform).

4.29 The Committee is also concerned about the disagreement between the AFP (basing its opinion on advice of the Commonwealth Director of Public Prosecutions) and the Attorney-General's Department (basing its opinion on advice of the Solicitor-General) on the current legal status of law enforcement agencies relying on section 3L of the *Crimes Act 1914*, to access remotely stored communications.

4.30 As a result of these conflicting positions, these provisions of the Bill do not offer the certainty that is needed in the important matters arising under the TI regime.

4.31 The Committee recommends that Parliamentary consideration of proposed subsections 6(1), 6(5), 6(6) and 6(7) be deferred, to allow these conflicting opinions between the Attorney-General's Department and the AFP to be resolved and Parliament to be informed of the outcome.

4.32 In regards to the other provisions of the Bill, specifically the extension of the crimes covered by the TI regime, removing the requirement that ASIO notify callers to publicly listed numbers that the call is being recorded, and removing the requirement that ASIO notify carriers of a TI warrant where no action is required on the part of the carrier, the Committee believes that an appropriate balance is met between protecting the interests of national security and protecting the privacy of individuals.

Recommendation 1

4.33 The Committee recommends that Parliamentary consideration of proposed subsections 6(1) 6(5), 6(6) and 6(7) 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 Bill.

Recommendation 2

4.34 The Committee supports the remaining provisions of the Bill, and the Committee recommends that the remainder of the Bill proceed.

Senator Marise Payne

Chair

Additional comments and points of dissent by Senator Brian Greig

The Australian Democrats unequivocally oppose the provisions in this Bill will which facilitate access to stored communications of delayed access message services without an interception warrant.

We note the following passages within the *Bills Digest*:

> "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".
>
> "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?"

The Democrats believe that the answer to this question is an emphatic "no".

We see no reason why electronic communications, such as SMS, email and voicemail should be treated any differently from telephone calls, simply because they can be stored and accessed at a later time.

The use of SMS, email and voicemail as means of communication is increasing rapidly and the Australian community should be able to reap the benefits of this technology without fearing Government access to their private communications.

The Democrats believe that these proposed changes will undermine the fundamental purpose and intent of the Telecommunications (Interception) Act and will enable unjustifiable infringements of personal privacy.

We support the Committee's first recommendation that the consideration of subsections 6(1), 6(5), 6(6) and 6(7) be postponed until Parliament has been informed of any agreement between the Attorney-General's Department and the Australian Federal Police regarding the current operation of the TI regime and how it will operate under the Bill.

However, we would go further and recommend that subsections 6(5) to 6(7) not be passed in any event. As long as those subsections remain in this Bill, we will strongly oppose it.

Senator Brian Greig
Australian Democrats

APPENDIX 1

ORGANISATIONS AND INDIVIDUALS THAT PROVIDED THE COMMITTEE WITH SUBMISSIONS

1	Electronic Frontiers Australia Inc.
2	Australian Privacy Foundation
3	Confidential
4	Optus
5	Office of the Victorian Privacy Commissioner
6	Attorney-General's Department
6A	Attorney-General's Department
6B	Attorney-General's Department
6C	Confidential
6D	Attorney-General's Department
6E	Attorney-General's Department
7	Australian Federal Police
7A	Australian Federal Police
8	NSW Minister for Police
9	Tasmanian Police

APPENDIX 2

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

Canberra, Monday 22 March 2004

Electronic Frontiers Australia Inc.

Ms Irene Graham, Executive Director

Australian Federal Police

Mr John Lawler, Acting Deputy Commissioner

Mr Rudi Lammers, Manager, Technical Operations

Mr John Ryles, Manager, IT

Mr Mike Phelan, Acting National Manager, Border and International Network

Attorney-General's Department

Mr Keith Holland, Assistant Secretary

Ms Anna Tearne, Principal Legal Officer

Mr Stuart Woodley, Senior Legal Officer

Ms Catherine Smith, Principal Legal Officer