The Senate

Legal and Constitutional Legislation Committee

Provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004

July 2004

ISBN 0 642 71426 6

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

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 A. Ridgeway, AD, NSW
Senator Natasha Stott Despoja, AD, SA
Senator Tsebin Tchen, LP, VIC
Senator John Tierney, LP, NSW
Senator John Watson, LP, TAS

Secretariat

Mr Phillip Bailey	Acting Secretary
Ms Alison Kelly	Senior Research Officer
Ms Marina Seminara	Executive Assistant

Suite S1.61 Telephone: (02) 6277 3560 Fax: (02) 62775794
Parliament House E-mail: legcon.sen@aph.gov.au

TABLE OF CONTENTS

ABBREVIATIONS

AFP	Australian Federal Police
EFA	Electronic Frontiers Australia Inc.
ISPs	Internet Service Providers
LEA	Law enforcement agency
SMS	Short Messaging Service
The Act	*Telecommunications (Interception) Act 1979*
The Bill	Telecommunications (Interception) Amendment (Stored Communications) Bill 2004
The first 2004 Bill	Telecommunications (Interception) Amendment Bill 2004
The 2002 Bill	Telecommunications Interception Legislation Amendment Bill 2002
TI Warrant	Telecommunications interception warrant
VOIP	Voice Over Internet Protocol

CHAPTER 1

INTRODUCTION

1.1 On 16 June 2004, the Senate referred the provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 to the Senate Legal and Constitutional Committee for inquiry and report by 22 July 2004.

Key provisions of the Bill

1.2 The Bill amends the Telecommunications (Interception) Act 1979 (the Interception Act) to change the way in which the Interception Act applies to stored communications. The measures in the Bill will exclude interception of stored communications from the prohibition against interception. The amendments will have the effect of limiting the prohibition against interception to the "live" or "real time" interception of communications transiting a telecommunications system. The Bill contains a 12 month "sunset clause" beginning from the date of commencement.[1]

Conduct of the inquiry

1.3 The Committee wrote to over 60 individuals and organisations inviting submissions by 28 June 2004. Details of the inquiry, the Bill and associated documents were also placed on the Committee's website.

1.4 The Committee received 13 submissions and 2 supplementary submission; 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 a public hearing in Canberra on 1 July 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.

---

1 Proposed subsection 2(3).

CHAPTER 2

BACKGROUND TO THE BILL

2.1 This chapter briefly outlines the background to the proposed amendments and the main provisions of the Bill.

Background

2.2 The Bill is the third piece of proposed legislation that seeks to clarify the application of the *Telecommunications (Interception) Act 1979* (the Act) to stored communications that has been considered by the Senate Legal and Constitutional Legislation Committee.

2.3 The Telecommunications Interception Legislation Amendment Bill 2002 (the 2002 Bill), if enacted, would have removed the requirement for a TI warrant, where a stored communication could have been accessed without the use of a telecommunications line (except to the extent that such use is for turning on the equipment). The Committee recommended that the Attorney-General review the current law on access to stored communications with a view to amending the Telecommunications Interception Legislation Amendment Bill 2002 so that the accessing of such data requires a TI warrant. Those particular provisions of the Bill were withdrawn.

2.4 The Telecommunications (Interception) Amendment Bill 2004 (the first 2004 Bill), was similar to the 2002 Bill, however it sought to differentiate between those messages that had been accessed, and those that had not. If enacted, a stored communication could have been accessed without a TI warrant, if it could be accessed without use of a telecommunications line (except to the extent that this was for turning on the equipment) and it had been accessed by the intended recipient. It would also have removed the need for a TI warrant, where the intended recipient had not accessed the message, but access could be gained with equipment that the intended recipient could have used, and this did not require the use of a telecommunications line (except to the extent that this was for turning on the equipment).

2.5 The Committee heard evidence that practical difficulties could arise, from the fact that internet service providers (ISPs) are often unable to determine whether or not a message has been accessed. The Committee also heard conflicting evidence from the AFP and Attorney-General's Department as to whether section 3L of the *Crimes Act 1914* permitted the AFP to remotely access stored communications without a TI warrant. The Committee recommended that consideration of those aspects of the Bill relating to stored communications be deferred until there was agreement between the Attorney-General's Department and the AFP on the operation of the TI regime, and how it would operate under the Bill.

2.6 The Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 (the Bill), would have the effect that a TI warrant would not be required to access a stored communication, excluding those communications that are either Voice Over Internet Protocol (VOIP), or any other communication stored on a highly transitory basis as an integral function of the technology used in its transmission (eg momentary buffering). If enacted, the Bill would remove the need for a TI warrant, where a person has legal physical access to a stored communication, whether or not the intended recipient has accessed it.

Provisions of the Bill

Exception to prohibition against interception

2.7 Item 3 of the Bill would insert a new paragraph 7(2)(ad) into the Act. This would provide that the prohibition against interception would not apply to or in relation to the interception of a 'stored communication'. The exception would have effect for a period of 12 months from the date of commencement.[1] A 'stored communication' is defined as a communication that is stored on equipment or any other thing, but does not include Voice over Internet Protocol (VOIP) or any communication stored on a highly transitory basis as an integral function of the technology used in its transmission.[2]

2.8 The Bill would have effect for 12 months, and the Attorney-General has proposed that within this time a review of the Act will be conducted. In his second reading speech, the Attorney-General explained:

> These measures represent immediate and practical steps to address the operational issues faced by our law enforcement and regulatory agencies.
>
> However, the amendments also recognise the need for a more comprehensive review of access to stored communications and the contemporary relevance of Australia's interception regime.
>
> That is why the amendments will cease to have effect 12 months after their commencement.

---

1 Proposed paragraph 7(2)(ad)

2 Proposed subsection 7(3A)

> The government recognises that a broader review of access to modern means of communication is required.
>
> That is why I have asked my department to conduct a comprehensive review of the Telecommunications (Interception) Act and to report back to me before the expiration of these amendments.[3]

3 The Hon. Philip Ruddock MP, Attorney-General, *House of Representatives Hansard*, 27 May 2004, p.29,309.

CHAPTER 3

Key Issues

3.1 Many of the parties who contributed to the first 2004 Bill inquiry again expressed concern and opposition to the Bill. Those parties who supported the Bill in the last inquiry also supported the current Bill.

3.2 This chapter discusses the issues raised in submissions and evidence given during the public hearing in relation to the provisions of the Bill.

The need for the Bill

Clarification of law relating to the access of stored communications

3.3 Submissions supporting the Bill argued that the Bill is necessary to clarify the application of the *Telecommunications (Interception) Act 1979* (TI Act) to the interception of stored communications.[1]

3.4 Most arguments surrounding the need for clarification related to the fact that the TI Act was enacted before the development of email and SMS, and as a result is silent on the issue of stored communications. The Action Group into the Law Enforcement Implications of Electronic Commerce stated in its submission:

> The TI Act was enacted prior to many forms of communication that are now considered commonplace. Equally importantly, it was enacted prior to the convergence of many previously discrete technologies (for example, email or SMS messages used not only as replacement for a telephone call, but also to replace postal services). There is currently nothing in the TI Act that specifically addresses the manner in which stored communications should be dealt with. This situation has given rise to debate and various opinions on how the TI Act should apply to these newer forms of communication.[2]

3.5 The Australian Federal Police (AFP) explained the need for such clarification at the hearing:

> It is important to the detection and prosecution of offences that AFP officers are able to search the content of computers and to gain access to stored communications expeditiously. The AFP raised these and other imperatives

---

1 Australian Securities and Investments Commission, *Submission 4*, p.2.; Action Group into the Law Enforcement Implications of Electronic Commerce, *Submission 5*, p.1.;Western Australia Police Service, Office of Deputy Commissioner, *Submission 11*, p.1.; Tasmania Police Service, *Submission 12*, p.2.; Commonwealth Director of Public Prosecutions, *Submission 13*, p.1.

2 Action Group into the Law Enforcement Implications of Electronic Commerce, *Submission 5*, pp.1-2.

> during the committee's previous inquiries into proposed telecommunication amendments. The amendments proposed in the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 will clarify that a telecommunications interception warrant is not required to access stored communications such as voice and email.
>
> ...
>
> The AFP welcomes this clarification and the practical solution that it provides for the effectiveness of investigations into serious Commonwealth offences, such as terrorism and people-smuggling. From the AFP's operational perspective, the amendments will ensure that investigators are not required to obtain two warrants to conduct a single search. AFP concerns about the two-warrant scenario centred on the potential that important evidence could be put at risk. Without the amendment allowing expeditious access to stored communications, highly disposable and easily destroyed forms of evidence could have been lost during the time taken to access the requirements to obtain TI warrants. Obtaining TI warrants as a matter of course prior to every search would have resulted in an unnecessary and onerous burden on limited Commonwealth resources.[3]

3.6 The Music Industry Piracy Investigations Pty Limited (MIPI) stated in correspondence to the Committee that the ability of copyright infringers to hide their identity has made the enforcement of intellectual property rights increasingly reliant on access to information and data held at Internet service providers (ISPs).[4]

3.7 The Australian Securities and Investment Commission (ASIC) explained in its submission that there are differing views amongst ISPs as to whether they can produce unread emails when a search warrant is executed on them:

> In ASIC's view, the application of the current provisions of the TI Act to forms of communication such as email and voicemail is unclear. The TI Act is a relatively old piece of legislation (passed in 1979) and so there is some difficulty in applying its language to more recent phenomena such as email. As a consequence, [there is] a great deal of confusion throughout the internet industry as to what form of communications can be seized under a conventional search warrant or compulsory notice and what forms of communications require a telecommunications interception warrant. Understandably, some internet service providers feel it best to err on the side of caution and refuse production to a wide range of communications including some forms of communication to which ASIC believes it has a right of access. This approach has impacted on ASIC investigations.[5]

---

3 *Committee Hansard*, 1 July 2004, p.17.

4 Correspondence of Music Industry Piracy Investigations Pty Limited, 7 July 2004, p.5.

5 Australian Securities and Investments Commission, *Submission 4*, p.2.

3.8 Ms Irene Graham of EFA addressed this issue in the hearing, and argued that if agencies such as ASIC believe that they do not have sufficient powers when executing search warrants then such powers should be specifically granted, as opposed to providing a general exception:

> If ASIC does not feel it has sufficient powers at the moment to access whatever it is it needs to access then I think it is a matter for ASIC to convince the government and the parliament that it needs greater powers for specific reasons. Those specific reasons should be identified in the same way that serious crimes are identified in the Telecommunications (Interception) Act. The serious risk is this. Even if one says that perhaps in some circumstances ASIC should be able to do this or that, this bill is not just dealing with ASIC's perceived problems; it is granting a vast number of agencies increased powers.[6]

3.9 In the Committee's consideration of the first 2004 Bill, the Committee received conflicting opinions from the AFP and the Attorney-General's Department as to how the TI Act interacted with section 3L of the *Crimes Act 1914*, in terms of whether the AFP needed a TI warrant to access remotely stored communications.[7]

3.10 On the basis of these conflicting opinions the Committee recommended that the provisions of the Bill relating to stored communications be deferred until Parliament was informed of agreement between the AFP and the Attorney-General's Department on the operation of the TI regime.[8]

3.11 In the hearing for the current Bill, a representative of the AFP explained that if enacted, the Bill would clarify the issue for the purposes of its operations.[9] This point was supported by a representative of the Attorney-General's Department.[10]

Support of information technology security and integrity

3.12 The first 2004 Bill would have distinguished between read and unread emails. During the Committee's consideration of that Bill, the AFP objected to those provisions, on the grounds that this would have limited its ability to perform information technology security and integrity measures which involved accessing un-

---

6 *Committee Hansard*, 1 July 2004, p.20.

7 Senate Legal and Constitutional Legislation Committee, "Provisions of the Telecommunications (Interception) Amendment Bill 2004", March 2004, pp.16-17

8 Senate Legal and Constitutional Legislation Committee, "Provisions of the Telecommunications (Interception) Amendment Bill 2004", March 2004. p.27, Recommendation 1.

9 *Committee Hansard*, July 1 2004, p.20.

10 *Committee Hansard*, July 1 2004, p.25.

read emails (as this would have constituted an 'interception' and required a TI warrant).[11]

3.13 The current Bill does not make a distinction between read and unread emails, and allows access to all stored communications. In light of this, the AFP argued in its submission that the Bill will resolve corporate governance concerns, where human intervention is required in scrutinising email communications to members.[12]

3.14 The Action Group into the Law Enforcement Implications of Electronic Commerce also supported this consequence of the Bill:

> Both public and private sector agencies generally undertake active programs of email scanning for malicious code, inappropriate content, and anything else specified as contrary to the agency's 'acceptable use' policy. Such scanning processes generally involve machine reading or viewing, with the human element required to make a final determination in some instances.
>
> By allowing access at the storage destination, or through permission, the proposed amendments will ensure that agencies undertaking this important e-security work will not inadvertently breach the TI Act.[13]

3.15 The Office of the Federal Privacy Commissioner responded to this argument in its submission, proposing that if such integrity measures are needed, the TI Act could be amended to give a limited exemption for such purposes, instead of making a general exemption:

> If there is continued uncertainty about whether such activities may contravene the Interception Act, this could be resolved by amending the legislation to ensure that while protection is maintained for personal telecommunications generally, e-security and corporate governance measures are permitted.[14]

3.16 At the hearing, the AFP were asked to respond to this suggestion, and acknowledged that this issue could be addressed by making such an amendment to the TI Act.[15]

---

11 Senate Legal and Constitutional Legislation Committee, "Provisions of the Telecommunciations (Interception) Amendment Bill 2004", March 2004. p.9.

12 Australian Federal Police, *Submission 7*, pp.1-2.

13 Action Group into the Law Enforcement Implications of Electronic Commerce, *Submission 5*, p.2.

14 Office of the Federal Privacy Commissioner, *Submission 6*, p.3.

15 *Committee Hansard*, 1 July 2004, p.21.

The Committee's view

3.17 The Committee notes that unlike the first 2004 Bill, the current Bill does not seek to differentiate between 'stored communications' that have been accessed and those that have not. In examining the first 2004 Bill, the Committee heard evidence that it is often not possible for an ISP to determine whether an email has been accessed or not.

3.18 On the other hand, during the inquiry into the current Bill, Ms Graham said:

> …I am told that the newer versions of software make this markedly easier for ISPs to know and… I understand, even with the older software, that at least they were able to know whether the subject line and the 'from' field, for example, had been seen on a web page. I may be mistaken about that, but I am told that technology has moved along in this. I would be extremely surprised if businesses like Telstra and BigPond – all of those major ISPs – were not able to identify whether messages had at least been accessed by the subject lines being viewed on a computer screen.[16]

3.19 It is apparent that there remains uncertainty about whether ISPs can identify whether a message has been accessed by its intended recipient. I would be desirable if the review of the Act proposed by the Attorney-General in his second reading speech examined this issue in more detail.

3.20 Whilst allowing both read and unread 'stored communications' to be accessed may raise privacy concerns that might not have been as apparent in the first 2004 Bill, it does mean that unlike that Bill, the current Bill will be able to be applied with certainty. In that regard, the concerns of the Committee over the uncertainty inherent in the first 2004 Bill are satisfied.

3.21 The Committee is also satisfied that the actions of agencies such as the AFP who seek to review the content of ingoing and outgoing emails for the purposes of professional standard and IT security screening will be clearly permitted by this Bill. Notwithstanding this, the Committee notes that the need for agencies such as the AFP to undertake such screening could also be achieved through amending the TI Act to provide specific exemptions. It is issues such as this that should be considered in any review of the TI regime as was proposed by the Attorney-General in his second reading speech.

Concerns expressed about the Bill

3.22 Submissions opposed to the Bill expressed three major concerns:

- Privacy issues regarding the accessing of un-read stored messages without a telecommunications interception warrant;

---

16 Ms Irene Graham, *Committee Hansard*, 1 July 2004, p.5.

- Search warrants do not offer the same protections as TI warrants; and
- The Bill does not require or detail a review of the TI regime

Accessing un-read stored messages

3.23 Submissions that opposed the Bill expressed concern that the Bill would offer less privacy protections than what would have been offered by either the 2002 Bill or the first 2004 Bill.[17] Specific concern related to the fact that the Bill would exempt the access of stored communications from the TI regime, whether or not they had been read.

3.24 EFA argued that if the Bill is enacted, it would no longer be illegal for anyone, (not just law enforcement agencies (LEAs)) to access unread stored communications. It further argued that if enacted, the Bill would remove from the Act the prohibition on employees of telecommunications service providers from spying on customers' electronic communications during their passage.[18] EFA argued that the need for parties to maintain network security should not be used as a basis for allowing telecommunication service providers to access customer stored communications:

> There is a vast difference between allowing employers to manage their own internal communications systems and allowing telecommunications servicer providers' employees to have unfettered access to trawl through their customers' temporarily delayed and stored communications without the customer's knowledge and permission.[19]

3.25 This argument was challenged by MIPI, who noted that many ISP customers are required to consent to ISPs capturing and disclosing communications held by the ISP under standard terms and conditions:

> Ordinarily ISP customers have already consented to the capture and disclosure of information and communications held by the ISP under their standard terms and conditions… ISPs themselves routinely exercise their contractual rights to record information including communications for their own use and to disclose them to law enforcement agencies, without reference to their customers.[20]

---

17 Australian Privacy Foundation, *Submission 1*, p.2; Electronic Frontiers Australia, *Submission 2*, p.2.; Office of the Victorian Privacy Commissioner, *Submission 3*, p.1.

18 Electronic Frontiers Australia, *Submission 2*, p.8.

19 Electronic Frontiers Australia, *Submission 2*, p.9.

20 Correspondence of Music Industry Piracy Investigations Pty Limited, 7 July 2004. p.8.

3.26 EFA were also concerned that if the Bill was enacted, sections 280 and 282 of the *Telecommunications Act 1997* would allow some agencies to access stored communications at an ISP without a search warrant.[21]

3.27 EFA noted that paragraph 280(1)(b) of the *Telecommunications Act 1997* permits disclosure or use of information or a document if that is required or authorised by law:

> This broad term includes statutory, judicial and quasi-judicial powers, such as court orders made during the discovery process, summons for witnesses to attend and produce records and subpoenas for documents.[22]

3.28 It further noted that subsections 280(1) and (2) of the *Telecommunications Act 1997* permit carriers and carriage service providers (including ISPs) to disclose documents and information to agencies on request without a warrant if the service provider considers the disclosure or use is "reasonably necessary" for the enforcement of the criminal law.[23] It noted that section 282 is often used to obtain call charge records:

> Section 282 is very frequently used to obtain call charge records etc. It enables disclosure of information such as customer identification details and the source, path and destination of communications (for example, telephone numbers dialled, and the "To" and "From" fields of an email message, etc). In the 2002-2003 year, 400,766 disclosures of information or documents were made to government agencies under s282(1) and (2) of the *Telecommunications Act* (i.e. without a warrant or certificate) by telecommunications carriers, carriage service providers (includes ISPs) or number database operators. This is 60% of the total disclosures (666,521) under Part 13 of that Act.[24]

3.29 Pursuant to section 309 of the *Telecommunications Act*, the Federal Privacy Commissioner has a role in monitoring compliance by telecommunications service providers with their obligations under the *Telecommunications Act* to keep records of disclosures under these provisions. The Committee notes with concern the evidence of the Acting Federal Privacy Commissioner that:

> With the work of the Office of the Federal Privacy Commissioner's compliance section currently focussed on complaint handling, it is not carrying out audits in a range of areas, including under this provision.[25]

---

21 Electronic Frontiers Australia, *Submission 2*, p.11.

22 Electronic Frontiers Australia, *Submission 2*, p.11.

23 Electronic Frontiers Australia, *Submission 2*, p.12.

24 Electronic Frontiers Australia, *Submission 2*, p.13.

25 Office of the Federal Privacy Commissioner, *Submission 11*, p.2.

3.30 The Committee has heard such evidence on numerous occasions during the Estimates process and suggests that this problem assumes greater urgency in light of the provisions of this Bill.

3.31 At the hearing, a representative of ASIC stated that it believes it currently has the power to use compulsory notices to gain access to read emails stored at an ISP, but that ISPs do not share this view, and that:

> …[ISPs] err on the side of caution. ISPs, particularly the large ones that I have been dealing with, believe that—and this is a general statement—the situation is unclear and, until such time as clarity is provided, they are going to err on the side of caution and will ask for interception warrants.[26]

3.32 The representative from ASIC also noted that whilst ASIC believes it has the power to use compulsory notices to access emails at an ISP if they have been read, it has been advised by the Attorney-General's Department that it does not have the power to do so if the email has not been read. However, it was noted that a problem arises when ISPs are unable to determine with certainty whether an email has been read or not, and therefore they decline to respond.[27]

3.33 The representative of ASIC went on to note that in its view, if the Bill was enacted, ASIC would be able to use compulsory notices to access all emails stored at an ISP, whether they had been read or not:

> At least some of our compulsory notice powers are quite restricted in terms of what we could require production of, but they do not actually require that an offence has been committed or that we have suspicion that an offence has been committed before we can serve them. To clarify my previous response, I think that that is correct except in cases where the email is still in transit and is basically bouncing from computer to computer before it reaches its final home. In those cases this bill would not allow us to access those, because that is subject to an exception under the provision.[28]

3.34 It was explained that ASIC has various guidelines and checks and balances in place regarding its access powers:

> Our notices can be challenged and are regularly challenged in court as to the propriety of their content. We are regularly asked to substantiate our notices and we do that with very high success rates. We also have record-keeping guidelines that ensure continuity of evidence. From the moment that evidence or potential evidence comes into our hands it is logged and stored.

---

26 *Committee Hansard*, 1 July 2004, p.9.

27 *Committee Hansard*, 1 July 2004, p.10.

28 *Committee Hansard*, 1 July 2004, p.10.

> Our access powers to information are also reviewable by the Privacy Commissioner. ASIC has been subject to a number of privacy audits around the country by the Privacy Commissioner's staff over the years, specifically reviewing and auditing the propriety of our information collection and our evidence collection. We are also reviewable. Many of our decisions are reviewable—our administrative decisions under the AAT—and those reviews can also look at the propriety of our access to documentation. There are many layers of review and supervision of ASIC's access powers, including not least the ability to challenge our notices in the court.[29]

3.35 The Acting Federal Privacy Commissioner was asked at the hearing to comment on these safeguards:

> We certainly understand that ASIC has considerable guidelines in place, as was mentioned by the representatives of ASIC. We have done audits of their organisation in the past and on the whole through those audits we have been quite satisfied with the various protections for the personal information they collect. On that basis, we would not assume that they would be dramatically changing the protection of the personal information they collect.[30]

3.36 The Acting Federal Privacy Commissioner went on to state that his office would prefer to see the "higher" protections offered by the TI warrant regime in relation to such agencies accessing stored communications.[31]

3.37 The AFP also noted in their submission that they have internal procedures and regulation to ensure information is maintained and used properly:

> Australian Federal Police officers are bound by the Information Privacy Principles in the *Privacy Act 1988,* and may be subject to criminal sanctions relating to the unlawful disclosure of information (eg, section 60A of the *Australian Federal Police Act 1979* and section 70 of the *Crimes Act 1914*).
>
> All conduct undertaken by AFP members, including application and execution of search warrants, is subject to internal and external scrutiny. Complaints about an officer's conduct may be referred to AFP Professional Standards and independently to the Commonwealth Ombudsman. Depending on the outcome, dismissal or disciplinary action may ensue. Civil remedies and criminal action are also available.[32]

3.38 In a supplementary submission to the Committee, the Office of the Federal Privacy Commissioner noted that the *Privacy Act 1988* does not require agencies such

---

29 *Committee Hansard*, 1 July 2004, p.11.

30 *Committee Hansard*, 1 July 2004, p.13.

31 *Committee Hansard*, 1 July 2004, p.13.

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

as the AFP to destroy information about individuals that is not relevant to its functions or activities:

> The Information Privacy Principles (IPPs) in the *Privacy Act 1988* (the Privacy Act) apply to information about individuals handled by most Commonwealth agencies, including the Australian Federal Police (AFP).
>
> It is important to note in the context of the current Bill that the IPPs do not include a requirement to destroy data that is not relevant to an agency's functions or activities. This is in contrast, for example, to the National Privacy Principles (NPPs) that apply to the private sector (see NPP 4.2). Therefore, information about third parties may be able to be retained indefinitely by an agency.
>
> In light of this, the Committee may wish to consider whether there are adequate existing legislative obligations, in relation to the destruction of unnecessary or irrelevant personal information (for example, that not needed in an investigation), on agencies and others that might be permitted to collect information about third parties from stored communications, if the Bill is enacted.[33]

3.39 The Committee suggests that this issue is considered in the review of the Act.

3.40 Whilst agencies such as ASIC and the AFP have internal safeguards for protecting the privacy of information it collects, EFA expressed concern that if the Bill was enacted, private parties could use injunctions (such as Anton Pillar orders) to access stored communications, and they do not have equivalent internal safeguards:

> There is a situation in Australia at the moment where judges are granting orders to lawyers and private investigation agencies, particularly for the music industry, where the lawyers and private investigation agencies are able to go into individuals' homes, ISPs' offices and telephone companies' offices and take copies, under the court order, of the entire hard drive of computers in those premises.
>
> …
>
> That is clearly a major concern for us. At the moment, when these raids are conducted at the University of New South Wales, Telstra's premises and so forth we trust that a copy of the entire email server of the ISP is not taken because to do so would include copies of undelivered emails; therefore, it would be an illegal interception. If this bill passes, there will no longer be any restriction legislatively on whether or not those court orders—that is, Anton Pillar orders—can authorise the taking of an entire copy of an ISP's email server. We find that very concerning because that would be occurring without a warrant. Granted, it would be a court order, but these court orders are very broad. When you are taking a copy of an ISP's email server this has

33 Office of the Federal Privacy Commissioner, *Submission 6A*, pp.1-2.

> nothing to do with the suspects; this is the email of every single customer of that ISP. We really feel that, until the laws about access to computer hard drives and so forth are vastly improved to ensure privacy is protected, we need the existing restrictions to stop things like Anton Pillar orders being able to be granted for the whole email server of an ISP.[34]

3.41 MIPI argued that there are existing procedural safeguards to regulate the use of such court orders:

> [There are] stringent requirements for rights owners to obtain Court orders that permit the capture of electronic evidence, including emails. There is no evidence of abuse of these requirements.[35]

Protections offered by search warrants

3.42 The procedural safeguards of agencies such as ASIC and the AFP, and the requirement that physical access to an ISP still needs to be legal (eg through a search warrant) was relied on by those in support of the Bill as grounds that privacy would be protected.[36]

3.43 Those opposed to the Bill argued that search warrants do not accord the same protections as a TI warrant.[37]

3.44 EFA noted that the eligible judges and nominated members of the Administrative Appeals Tribunal who are authorised to issue interception warrants must comply with conditions of issue set out in the TI Act, and must ensure privacy is not unduly infringed. It noted that equivalent considerations are not required in the issue of search warrants, and that search warrants can be issued by a larger cohort.[38]

3.45 The Office of the Federal Privacy Commissioner also noted the reduced protections offered by search warrants as opposed to TI warrants:

> In the absence of these protections, the oversight and accountability of the handling of the personal information of third parties by law enforcement and

---

34 *Committee Hansard*, 1 July 2004, pp.6-7.

35 Correspondence of Music Industry Piracy Investigations Pty Limited, 7 July 2004. p.9.

36 Australian Securities and Investments Commission, *Submission 4*, p.2. Action Group into the Law Enforcement Implications of Electronic Commerce, *Submission 5*, p.2.; Commonwealth Director of Public Prosecutions, *Submission 13*, p.1.

37 Electronic Frontiers Australia, *Submission 2*, p.13; Office of the Victorian Privacy Commissioner, *Submission 3*, p.2.; Office of the Federal Privacy Commissioner, *Submission 6A*, p.2.

38 Electronic Frontiers Australia, *Submission 2*, p.13.

> other investigative agencies will be limited to a lesser accountability framework under the Telecommunications Act.[39]

3.46 The Office of the Victorian Privacy Commissioner argued that whilst it may be appropriate for search warrants to be used to access read emails stored at an ISP, a TI warrant should be required where the email has not been read.[40]

The Committee's view

3.47 The Committee notes with concern the arguments presented that if enacted, the Bill will remove privacy protection for those using emails or SMS. The Committee heard competing policy arguments. Those in favour of the Bill argue that a stored email is analogous to a letter (and like a PO Box should be accessible with only a search warrant), whilst those opposing the Bill argue it is more analogous to a phone call, and should be protected by the TI Act like a phone call.

3.48 In any review of the TI Act, as proposed by the Attorney-General, thorough consideration and examination should be given to such policy arguments. The review should also consider what accountability mechanism apply when agencies and other parties use some form of 'lawful authority' to access stored communications and whether these are adequate to protect the privacy of those using emails or SMS.

The Bill does not require or detail the review of the TI Act

3.49 The Bill contains a sunset clause of 12 months following its commencement. At this time it will cease to have operation. If the Bill were enacted, the Attorney-General has proposed that there would be a review of the TI regime to report before the expiry of the Bill.

3.50 It was pointed out in submissions that the Bill does not mention or detail this review, and as a result does not require that the review will be public.[41]

3.51 Submissions that commented on this argued that the review should be public and should call for submissions.[42]

---

39 Office of the Federal Privacy Commissioner, *Submission 6A*, p.2.

40 Office of the Victorian Privacy Commissioner, *Submission 3*, p.2.

41 Electronic Frontiers Australia, *Submission 2*, p.3; Office of the Federal Privacy Commissioner, *Submission 6*, p.3.

42 Ibid.

The Committee's view

3.52 The Committee believes that if enacted, the review proposed by the Attorney-General should be public, and should call for submissions. The report of the review should also be public. The Committee believes that this should be specified in the Bill.

Conclusion

3.53 The Committee is satisfied that the Bill will clarify the law in relation to the access of stored communications, where a party has lawful access. The Committee acknowledges that the Bill will allow any party who has lawful access to a stored communication, to access it without the need for a TI warrant.

3.54 The Committee believes that there is a genuine need to ensure clarity as to the application of the TI Act to stored communications. If enacted, the Bill will achieve this clarity, although it will cease to have effect 12 months after its commencement. The Committee regards this as an important check in the process. The Committee believes that if the Bill is enacted, the review that is to take place within this 12 months should be public, and should reconsider the appropriateness of continuing the exemption of read and unread stored communications from the TI regime, as proposed in the Bill. The Committee has identified a range of issues in its report which bear upon this question.

3.55 To ensure that such a review does take place if the Bill is enacted, the Committee recommends that the Bill be amended to specifically require that such a review is conducted and is made public.

Recommendation 1

3.56 The Committee recommends that the Bill be amended to require that a review of the *Telecommunications (Interception) Act 1979* be undertaken and to specify that this review consider the issue of whether stored communications should be exempt from the Act. It should also require that the review publicly seek submissions and make its findings public. Subject to this amendment the Committee recommends that the Bill proceed.

Senator Marise Payne

Chair

DISSENTING REPORT BY THE AUSTRALIAN DEMOCRATS

1.1 The Australian Democrats do not share the Committee's view that the *Telecommunications (Interception) Amendment (Stored Communications) Bill 2004* ("the Bill") should be passed.

1.2 There are a number of points that we would like to make in relation to the Bill as follows.

Need for Legislative Clarification

1.3 The Democrats do acknowledge that there is a need for legislative clarification in relation to the application of the *Telecommunications (Interception) Act* ("the Act") to stored communications.

1.4 The Act was passed in 1979, well before email, SMS and voicemail services became available, and as a consequence there is some uncertainty as to how it applies to those services.

1.5 The Democrats have previously made representations to the Attorney-General's office regarding the need for legislative clarification in this area. Although we do not agree with the provisions of the Bill, we do believe that there is a need to provide clarification one way or the other.

1.6 There is evidence to suggest that the Act has previously been interpreted in way which enables agencies to access stored communications without an interception warrant. In this respect, the amendments could be said to provide legislative certainty to the way in which the Act is currently being interpreted.

1.7 However, the Democrats do not agree with this interpretation of the Act. For this reason, we regard the amendments proposed in the Bill as *changing* the current regime, rather than providing further clarification. Of course, it is the prerogative of the Parliament to make such changes if there are strong justifications for them.

Sunset and Review:

1.8 The Democrats welcome the inclusion of a sunset clause in the Bill, however we note that there is no obligation to destroy any information obtained under the Bill during its 12 months of operation. We also welcome the Attorney-General's undertaking that he will instigate a review of the legislation prior its expiration, but we agree with the recommendation of the Committee that this should be expressly provided for in the terms of the legislation.

The Right to Privacy

1.9 Under this Bill, however, Australian intelligence and law enforcement agencies will, for the first time, be able to access certain forms of telecommunications – namely SMS, email and voicemail – without an interception warrant.

1.10 The Democrats believe that individual Australians have the right to communicate privately with their friends, their families and their loved ones. Similarly, in a business context, Australian workers have the right to communicate privately with their employers, employees, colleagues and clients.

1.11 Human beings are continually developing new and innovative ways of communicating with each other and it is important that Australians have the freedom and the confidence to embrace these new technologies, without fear of Government surveillance. New technologies do not justify increased surveillance.

1.12 The Democrats do not believe that there is any policy justification for exempting email, SMS and voicemail from the prohibition against telecommunications interception. These are forms of communication which are used interchangeably in everyday practice with "live" telecommunications. For example, a person who telephones another person but is unable to get through, might leave a voicemail message, setting out the exact information they would have communicated directly to the person, had they been able to get through to them.

1.13 The Democrats do not believe it is in the interests of the Australian community to create disincentives for using such technology, which has the potential to promote greater efficiency within the Australian community.

1.14 This legislation provides a disincentive for the use of such technology because Australians will know that if they use such technology, their communications will not be afforded the same level of protection that they would if they spoke directly with others over the telephone.

1.15 The Democrats do not agree that stored communications can or should be compared to letters. Even email is clearly distinguishable from hard correspondence. For example, it can be sent to multiple recipients at once; it can be sent secretly to some recipients, without the knowledge of other recipients; and, senders can be notified when a recipient reads their email.

1.16 To the greatest extent possible, Australians should be at liberty to embrace these new technologies without the fear of serious intrusions on their privacy. Legislation in this instance should promote technological progress, not create reasons for Australians to revert to less efficient means of communication.

1.17 For all of the reasons, the Democrats take the view that the Act should be amended so that it expressly requires a telecommunications warrant to be obtained in order to access stored communications.

Senator Brian Greig

APPENDIX 1

ORGANISATIONS AND INDIVIDUALS THAT PROVIDED THE COMMITTEE WITH SUBMISSIONS

1 Australian Privacy Foundation

2 Electronic Frontiers Australia Inc.

2A Electronic Frontiers Australia Inc.

3 Victorian Privacy Commissioner

4 Australian Securities and Investments Commission

4A Australian Securities and Investments Commission

5 Action Group into the Law Enforcement Implications of Electronic Commerce

6 Office of the Federal Privacy Commissioner

6A Office of the Federal Privacy Commissioner

7 Australian Federal Police

8 Confidential

9 Law Institute of Victoria

10 Telestra Corporation Limited

11 Office of Deputy Commissioner

12 Tasmanian Police Service

13 Commonwealth Director of Public Prosecutions

Published correspondence

Correspondence of the Northern Territory Police, Commissioner's Office, 13 July 2004.

Correspondence of Music Industry Piracy Investigations Pty Limited, 7 July 2004,

APPENDIX 2

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

Canberra, Thursday 1 July 2004

Electronic Frontiers Australia Inc.
Ms Irene Graham, Executive Director

Australian Securities and Investments Commission
Mr Keith Inman, Director, Law Enforcement Unit
Ms Nicole Pyner, Manager, Enforcement Policy & Practice

Federal Privacy Commissioner
Mr Timothy Pilgrim, Acting Commissioner
Mr Paul Armstrong, Acting Deputy Privacy Commissioner

Australian Federal Police
Mr Trevor Van Dam, Chief Operating Officer
Federal Agent Rudi Lammers, Manager Technical Operations
Federal Agent Brian Olsen, Manager Information Technology

Federal Agent Kylie Weldon
Federal Agent David Batch

Attorney-General's Department
Mr Peter Ford, Acting Deputy Secretary, Criminal Justice and Security Group
Mr Keith Holland, Acting First Assistant Secretary, Information and Security Law Division
Ms Anna Tearne, Principal Legal Officer, Security Law Branch