The Senate

Legal and Constitutional Legislation Committee

Provisions of the Telecommunications (Interception) Amendment Bill 2006

March 2006

ISBN 0 642 71635 8

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 Patricia Crossin, **Deputy Chair**, ALP, NT # ^
Senator Andrew Bartlett, AD, QLD *
Senator Linda Kirk, ALP, SA
Senator Brett Mason, LP, QLD ^
Senator Nigel Scullion, CLP, NT

Substitute Members

* Senator Natasha Stott Despoja, AD, SA to replace Senator Andrew Bartlett for matters relating to the Attorney-General's Portfolio

\# Senator Annette Hurley, ALP, SA to replace Senator Patricia Crossin, ALP, NT for the Inquiry into the provisions of the Australian Citizenship Bill 2005 and a related bill

^ Senators Bishop, ALP,WA and Trood, LP, NSW to replace Senators Crossin, ALP, NT and Mason, LP, QLD for the Inquiry into the Defence Legislation Amendment (Aid to Civilian Authorities) Bill 2005 respectively

Participating Members

Senator the Hon. Eric Abetz, LP, TAS
Senator Lyn Allison, AD, VIC
Senator G. Barnett, LP, TAS
Senator Mark Bishop, ALP, WA
Senator George Brandis, LP, QLD
Senator Bob Brown, AG, TAS
Senator George Campbell, ALP, NSW
Senator Kim Carr, ALP, VIC
Senator Grant Chapman, LP, SA
Senator the Hon R Colbeck, LP, TAS
Senator Stephen Conroy, ALP, VIC
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 Steve Fielding, FFP, VIC
Senator Concetta Fierravanti-Wells, LP, NSW
Senator the Hon Bill Heffernan, LP, NSW
Senator John Hogg, ALP, QLD
Senator Gary Humphries, LP, ACT
Senator Annette Hurley, ALP, SA
Senator Barnaby Joyce, NATS, QLD
Senator Ross Lightfoot, LP, WA
Senator Joseph Ludwig, ALP, QLD
Senator Kate Lundy, ALP, ACT
Senator the Hon Ian MacDonald, LP, QLD
Senator Julian McGauran, NPA, VIC
Senator Jan McLucas, ALP, QLD
Senator Christine Milne, AG, TAS
Senator Kerry Nettle, AG, NSW
Senator Stephen Parry, LP, TAS
Senator the Hon Kay Paterson, LP, VIC
Senator Robert Ray, ALP, VIC
Senator the Hon. Nick Sherry, ALP, TAS
Senator Rachel Siewert, AG, WA
Senator Ursula Stephens, ALP, NSW
Senator Russell Trood, LP, QLD
Senator John Watson, LP, TAS

Secretariat

Mr Jonathan Curtis	Secretary
Ms Rebecca Manen	Principal Research Officer
Ms Anne O'Connell	Principal Research Officer
Ms Marina Seminara	Executive Assistant

Suite S1.61	T: (02) 6277 3560	E: legcon.sen@aph.gov.au
Parliament House	F: (02) 6277 5794	W: www.aph.gov.au/senate_legal

TABLE OF CONTENTS

RECOMMENDATIONS

Recommendation 1

3.18 The Committee recommends that the Bill be amended to include a provision amending Section 280 and subsections 282(1) and (2) of the *Telecommunications Act 1997,* effective from the same date as the Bill, to make it clear that covert access to stored communications is not permitted without a stored communications warrant.

Recommendation 2

3.42 The Committee recommends that the enforcement agencies able to access stored communications should be limited to those agencies eligible under the existing arrangements for telecommunications interception.

Recommendation 3

3.43 The Committee recommends that the Bill be amended to permit stored communications warrants to be issued only in relation to criminal offences.

Recommendation 4

3.52 The Committee recommends that the Bill be amended to require applications for stored communications warrants, and the warrant itself, to include information that clearly identifies the person who will be the subject of the warrant and the telecommunications for which access is sought.

3.53 The Committee suggests that the existing provisions for named person warrants provide a suitable example of the type of information that ought to be required.

Recommendation 5

3.60 The Committee recommends that the Bill be amended to allow issuing authorities to only include those currently able to issue interception warrants.

Recommendation 6

3.67 The Committee recommends that, consistent with the existing arrangements for telecommunications interception, immediate action be taken to ensure the enforceability of the stored communications provisions on State and Territory agencies by requiring complementary legislation to be enacted as a precondition to being granted the powers of an enforcement agency under the stored communications regime.

Recommendation 7

3.68 The Committee also recommends that as an interim measure, the definition of an enforcement agency in the Bill be amended to allow for the ability to exclude an agency specified in the Telecommunications Interception Regulations from being able to obtain a stored communications warrant.

Recommendation 8

3.72 The Committee recommends that the Bill be amended to allow issuers of stored communications warrants to have regard to the length of time stored communications may have been held on a carrier's equipment and whether the communications sought can be sufficiently identified in order to minimise the impact on privacy.

Recommendation 9

3.73 The Committee also recommends that the Bill be amended to require issuers of stored communications warrants to consider whether the stored communications are likely to include communications the subject of legal professional privilege and whether any conditions may be implemented to prevent the disclosure of such communications.

Recommendation 10

3.81 The Committee recommends that the Bill be amended to specify time limits within which an agency must both review their holdings of information accessed via a stored communications warrant and destroy information as required under the proposed section 150.

Recommendation 11

3.91 The Committee recommends that Bill be amended to require agencies and the Minister to report on the use and effectiveness of stored communications warrants in a manner equivalent to the existing reporting obligations for telecommunications interception warrants.

Recommendation 12

3.92 The Committee recommends that additional resources be provided to the Ombudsman to enable the Office to fulfil the expanded functions under this Bill.

Recommendation 13

3.93 The Committee recommends that the Bill be amended to extend the timeframe for section 153 reports to six months.

Recommendation 14

3.107 The Committee recommends that the Bill be amended to ensure that copies of communications can not be accessed without a stored communications warrant.

Recommendation 15

3.108 The Committee recommends that the definition of 'record' be amended so that it applies in relation to accessing a stored communication.

Recommendation 16

3.109 The Committee recommends that the issue regarding whether or not access to stored communications is accessible via the sender is settled and the Bill be amended as necessary.

Recommendation 17

3.110 The Committee recommends that prior to the passage of the Bill the definition of stored communications be amended so that the Australian Communications and Media Authority's ability to enforce the Spam Act is not limited.

Recommendation 18

4.43 The Committee recommends that as a precondition to issuing a warrant under subsection 9(3), there must be evidence that the B-party's telecommunications service is likely to be used to communicate or receive information relevant to the particular activities prejudicial to security which triggered the warrant.

Recommendation 19

4.56 The Committee recommends that the Bill be amended to require that an applicant for a B-party warrant demonstrate:

- **evidence to support their belief that the information likely to be obtained from the intercept is material to the investigation; and,**
- **establish that it cannot be obtained other than by telecommunications interception or the use of a listening device.**

Recommendation 20

4.57 The Committee also recommends that the proposed section 46(3) (which contains the requirement that the issuing authority must not issue a B-party warrant unless he or she is satisfied that the agency has exhausted all other practicable methods of identifying the telecommunications services used) be amended to exclude the word 'practicable', to ensure that before a person is subject to a B-party warrant no other way of approaching the problem is available.

Recommendation 21

4.61 The Committee recommends that the Bill be amended to state that B-party interception warrants cannot be renewed. If further interception is required after a warrant expires, it must be the subject of a fresh application.

Recommendation 22

4.80 The Committee recommends that Schedule 2 be amended to provide that certain material obtained under a B-party warrant will be exempted from use under the legislation. This material should include bona fide communications between solicitor and client; clergy and devotee; doctor and patient and communications by the innocent person with any person other than the person of interest to the law enforcement agency.

Recommendation 23

4.81 The Committee further recommends that the Bill be amended to introduce defined limits on the use and derivative use of material collected by B-party warrant.

Recommendation 24

4.97 The Committee recommends that:

- **there should be strict supervision arrangements introduced to ensure the destruction of non-material content in any form;**
- **the number and justification of B-party intercept warrants should be separately recorded by the Agency Co-ordinator and reported to the Attorney General; and**
- **the use of such warrants should be separately reported to the Parliament.**

Recommendation 25

4.111 The Committee recommends that the Bill should include a provision for the provisions to expire in five years, with a review at that time or earlier.

4.112 The Review should encompass the broader issues surrounding the suitability and effectiveness of AAT members in the warrant issuing regime, together with consideration of ways in which the Act may be amended to take account of emerging technologies such as peer-to-peer technology.

Recommendation 26

4.126 The Committee recommends that the recommendation contained at paragraph 3.2.5 of the Blunn report be adopted, and priority given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.

Recommendation 27

5.25 The Committee recommends that the amendments proposed in Schedule 6 of the Bill be passed.

Recommendation 28

5.26 Subject to the amendments set out above, the Committee recommends that the Bill be passed.

CHAPTER 1

INTRODUCTION

1.1 On 1 March 2006, the Selection of Bills Committee referred the provisions of the *Telecommunications (Interception) Amendment Bill 2006* to the Legal and Constitutional Legislation Committee for inquiry and report by 27 March 2006.

1.2 The purpose of the *Telecommunications (Interception) Amendment Bill 2006* (the Bill) is to amend the *Telecommunications (Interception) Act 1979* to implement certain recommendations of the *Report of the Review of the Regulation of Access to Communications*, written by Mr Anthony Blunn AO (the Blunn Report).

Key provisions of the Bill

1.3 The Bill proposes to amend the Act to:

- establish a regime to govern access to stored communications held by a telecommunications carrier (Schedule 1);
- enable the interception of communications of a person known to communicate with a person of interest (Schedule 2);
- enable interception of telecommunications services on the basis of a telecommunications device (Schedule 3);
- remove the distinction between class 1 and class 2 offences for which telecommunications interception powers are available to law enforcement agencies (Schedule 4);
- remove the Telecommunications Interception Remote Authority Connection function currently exercised by the Australian Federal Police and transfer the associated warrant register function to the Department administering the legislation (Schedule 5); and
- make other necessary amendments to the Act to ensure the ongoing effective operation of the interception regime in Australia (Schedule 6).

1.4 Chapter 2 provides a more detailed overview of the provisions of the bill.

Conduct of the inquiry

1.5 The Committee wrote to over sixty individuals and organisations inviting submissions by 13 March 2006. Details of the inquiry, the Bill and associated documents were also placed on the Committee's website.

1.6 The Committee received 24 submissions including 4 supplementary submissions. These are listed at Appendix 1. Submissions were placed on the Committee's website for ease of access by the public.

1.7 The Committee held a public hearing in Sydney on Wednesday, 15 March 2006. A list of witnesses who appeared at the hearing is at Appendix 2 and copies of the Hansard transcript are available on the internet at http://www.aph.gov.au/handsard

Acknowledgement

1.8 The Committee thanks those organisations and individuals who made submissions and gave evidence at the public hearing. In particular, the Committee notes the extremely short time frame in which the inquiry was conducted, and the difficulty this imposes on individuals and organisations – particularly volunteer based ones – to consider the provisions of a complex piece of legislation.

Note on references

1.9 References in this report are to individual submissions as received by the Committee, not to a bound volume. References to Committee Hansard are to the proof Hansard. Page numbers may vary between the proof and the official Hansard transcript.

CHAPTER 2

OVERVIEW OF THE BILL

Background

2.1 The purpose of the *Telecommunications (Interception) Amendment Bill 2006* (the bill) is to amend the *Telecommunications (Interception) Act 1979* (the Act) to implement certain recommendations of the *Report of the Review of the Regulation of Access to Communications* (the Blunn Report).

2.2 A major feature of the bill concerns lawful access to stored communications. There have been previous attempts to amend the Act to achieve this. They include provisions in the Telecommunications Interception Legislation Amendment Bill 2002 which proposed access to stored communications without the requirement for a telecommunications interception warrant. These provisions were withdrawn following a recommendation from the Committee that 'an interception warrant should be required for access to such communications.'[1]

2.3 Again, in February 2004, the Telecommunications (Interception) Amendment Bill 2004 provided that a telecommunications interception warrant would be required to obtain access to material which had not been retrieved by the intended recipient. A Committee inquiry found that that Bill was unclear about access to stored communications. The inquiry also revealed a disagreement between the Attorney-General's Department and the AFP as to the state of the existing legislation in relation to stored communications. The Committee recommended that Parliamentary consideration of the proposed subsections dealing with stored communications be deferred until the disagreement was resolved and Parliament was informed of the outcome.

2.4 A further amendment proposal in 2004, (the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004*) provided an interim access regime for stored communications pending the outcome of the Blunn Report. The amendments were to expire on 14 December 2005, but on 14 September 2005, were further extended until 14 June 2006, to allow time for the Government to fully consider the recommendations from the Blunn Report.

Overview of the Bill

Schedule 1: Stored communications

2.5 The stored communications amendments prohibit access to stored communications held by a telecommunications carrier, subject to certain limitations.

---

1 Bills Digest No. 111 2003-04

Access to stored communications

2.6 The bill introduces a warrant regime for enforcement agencies to retrieve stored communications held by a carrier. The amendments regulate the use, communication and recording of information obtained by access to stored communications and require the enforcement agencies to report to the Minister regarding the use of the stored communications powers.

Applications for warrant

2.7 Warrants are only available to an enforcement agency which is investigating an offence punishable by a maximum period of imprisonment of three years or a pecuniary penalty of at least 180 penalty units ($19,800).

2.8 The existing interception warrant applications are limited to law enforcement agencies such as the AFP and the Australian Crime Commission. However, the bill proposals also permit applications to be made by all agencies responsible for administering a law imposing a pecuniary penalty or administration of a law relating to the protection of the public revenue. This includes the Australian Customs Service, the Australian Tax Office, and the Australian Securities and Investments Commission. Similar State and Territory agencies are also included.

Issue of warrants

2.9 Warrants are issued by an issuing authority appointed by the Minister and may include Judges of Courts exercising Federal jurisdiction, a Federal Magistrate, or a magistrate. The appointment is contingent upon the nominated person accepting the appointment in writing. The Minister may also appoint Members of the AAT who are legal practitioners of at least 5 years' standing.

Definition of stored communications

2.10 The proposed definition of stored communication **(item 1)** provides that a stored communication is a communication that, among other things, is held on equipment operated by the carrier at its premises. The explanatory memorandum states that:

> This is to ensure that, …, the stored communications regime only applies to accessing stored communications via a telecommunications carrier. The regime does not affect existing lawful access to communications stored on a person's telecommunication device.

Use of information obtained under a stored communications warrant

2.11 The use or communication of information which is obtained from stored communications will be limited to matters connected with investigating an offence which is punishable by a maximum period of imprisonment of one year, or a pecuniary penalty of at least 60 penalty units.

Schedule 2: Access to communications from third parties

2.12 Schedule 2 provisions enable agencies to obtain an interception warrant for communications of an associate of a person of interest. These have been called the 'B Party' interception warrants.

Application for and issue of warrants

2.13 The warrant may only be issued where the investigation involves serious offences that attract a maximum penalty of seven years imprisonment. The provision also requires the issuing authority to be satisfied that:

- there are reasonable grounds for suspecting that a particular person is using, or is likely to use, the telecommunications service;
- information that would be obtained by interception would be likely to assist in connection with the investigation by the agency of the seven-year offence in which the suspect is involved; and
- the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the suspect.

2.14 When issuing the warrant, the issuing authority must also have regard to the following:

- the extent to which the proposed interception interferes with the privacy of any person;
- the gravity of the offences being investigated;
- the extent to which the information obtained under the warrant will assist the investigation;
- the extent to which alternative methods of investigation have been used or are available to the agency; and
- the extent to which these alternative methods would be useful to or would prejudice the investigation.

2.15 The warrant applications are accompanied by an affidavit, sworn by the representative of the applicant agency. These are provided for half the time of existing interception warrants – 45 days for law enforcement authorities and 3 months for ASIO warrants.

Schedule 3: interception of telecommunications services on the basis of a telecommunications device

2.16 The existing TI warrants are 'named person warrants'. These amendments are 'equipment-based' rather than attaching to the person who is recorded as the owner of the service. This will allow access to mobile phone text messages, as well as voice messages.

2.17 The issuing authority must only issue a warrant under this part unless satisfied that the applicant agency 'has no practicable methods of identifying the telecommunications services used or likely to be used by the person of interest, or that interception of those services would not be possible'.[2]

2.18 The Explanatory Memorandum to the bill notes that this covers instances in which agencies may be able to identify all services, but it is impracticable to intercept each service. The example given is the person who uses multiple SIM cards to evade interception.

Schedule 4: Removal of references to Class 1 and Class 2 offences

2.19 The interception regime has until now authorised interception on the basis of classes of offences. In the past only Class 2 offences required the issuing authority to have regard to privacy considerations. The offence distinctions have been removed and the offences are now termed 'serious offences'. Serious offences are defined in the new section 5D, and include murder or similar offences, kidnapping, offences under Division 307 of the Criminal Code (these include importation and possession of certain drugs and plants) terrorism offences, offences against Division 72, 101, 102 or 103 of the Criminal Code (terrorism offences); or an offence in relation to which the ACC is conducting a special investigation.

2.20 The privacy considerations now apply to all interception warrants.

Schedule 5: Transfer of functions

2.21 The Schedule changes the arrangements concerning the Telecommunications Interception Remote Authority Connection, an electronic system which requires the interception agency to lodge its interception warrants with the AFP. The Explanatory Memorandum to the bill indicates that the system has outlived its usefulness, and is to be discontinued.

2.22 The effect of this will be to allow warrants once issued to be executable immediately, rather than having to wait for them to be registered with the AFP. Registers will be kept by the Secretary of the Attorney General's Department who will receive and review warrants on issue.

Schedule 6

2.23 These provisions are largely consequential, and provide for specific state application where necessary. In addition, the use of interception powers by security and law enforcement agencies continues to be subject to strict reporting, disclosure and destruction provisions of the Act.

---

2 Explanatory Memorandum, p.34

CHAPTER 3

STORED COMMUNICATIONS

Introduction

3.1 The principal consideration of legislation which governs access to personal communications should be the protection of privacy. However, it is accepted that in limited circumstances it may be in the public interest to allow access to such communications. It is therefore essential that any legislation permitting access to personal communications achieves an appropriate balance between preserving privacy and assisting law enforcement agencies to effectively investigate serious offences. The primary test must always be whether the seriousness of the offence being investigated sufficiently warrants a significant invasion of an individual's privacy. This is particularly important whenever access to information is by covert interception.

3.2 The proposed amendments create a general prohibition on access to stored communications subject to prescribed exceptions including a stored communications warrant. The effect of the general prohibition proposed in this Bill is to prevent law enforcement agencies from serving notices to produce to obtain stored communications from a carrier without the knowledge of the intended recipient.

3.3 The proposed amendments clarify the lawful position surrounding access to stored communications which has previously been under dispute. This includes the ability of enforcement agencies to use warrants pursuant to section 3L of the *Crimes Act*, or other lawful notices to produce, to covertly obtain stored communications.

3.4 Generally, the clarification of access to stored communications provided by the Bill has been welcomed as a necessary and significant improvement. However, a number of areas of concern regarding the proposed stored communications warrants, as well as some definitional issues have emerged in the submissions and evidence received by the Committee at the hearing. These issues are considered in the following sections.

Access to stored communications

3.5 Section 108 prohibits access to stored communications 'without the knowledge of the intended recipient of the stored communication.'[1] The Explanatory Memorandum states that:

> The requirement for knowledge also preserves the ability of law enforcement agencies to access stored communications held by a carrier where they do so with the knowledge of the intended recipient … The distinction means that enforcement agencies are regulated by the stored

1 Proposed subsection 108(1)(b)

> communications regime only when they are acting covertly in the access to these communications.[2]

3.6 Electronic Frontiers Australia (EFA) argue that enforcement agencies should not be permitted to use existing notices to produce at the carrier because 'there is no means by which the carrier can know whether or not the intended recipient has in fact been notified by the agency prior to disclosing the information.'[3]

3.7 EFA also suggest that there is a lack of clarity in the existing telecommunications legislation, in particular the interrelationship between the *Telecommunication (Interception) Act 1979* and the *Telecommunications Act 1997* regarding the authorisation of agencies to obtain the content of stored communications via compulsory notices to produce.

3.8 Section 280(1)(a) of the *Telecommunications Act 1997* provides for the disclosure of information if:

> … in a case where the disclosure or use is in connection with the operation of an enforcement agency – the disclosure or use is required or authorised under a warrant.

3.9 EFA state that:

> We believe that the Telecommunications Act overrides [the ability of agencies to submit compulsory notices to produce under their own legislation] and therefore, once the interception Bill is passed it will then override the Telecommunications Act and, as a result, civil penalty agencies and criminal penalty agencies will need to provide a warrant. There are not notice-to-produce provisions. [4]

3.10 However, during the Inquiry it was noted that there have been instances in the past where various government agencies have had differing views about the kinds of warrants they needed to access information from a carrier.[5]

3.11 Advice from ASIC indicates that, in their view, subsections 282(1) and (2) of the *Telecommunications Act 1997*, allows them to obtain stored communications using their notice to produce powers.[6]

3.12 The Attorney-General's Department supports the view that upon enactment of the proposed Bill, the position in relation to stored communications would be clarified and access to stored communications will only be permitted with a warrant.[7]

---

2 Explanatory Memorandum, p. 7-8.

3 Electronic Frontiers Australia, *Submission 3*, p. 24.

4 Ms Graham, *Committee Hansard*, 15 March 2006, p. 8.

5 Ms Graham, *Committee Hansard*, 15 March 2006, p. 8.

6 Australian Securities and Investments Commission, *Submission 13B*, p. 2.

Committee view

3.13 The Committee notes EFA's concern regarding the ability of a carrier to know whether or not the intended recipient has been notified of access to communications prior to the disclosure of such information. However, the Committee considers that there are means by which an enforcement agency can inform the carrier of notification to the intended recipient.

3.14 The Committee considers that distinction between overt and covert access to communications as provided for in the Bill, is a critical one. The Committee considers that covert access to communications must be subject to much tighter controls than overt access. Where access is covert, individuals have virtually no opportunity to protect privileged information or to challenge the grounds on which such access was granted.

3.15 Given that many law enforcement agencies will be unable to access a stored communications warrant for covert access to stored communications, the Committee recognises the need of enforcement agencies to have an overt means of access. This requirement is satisfied through the ability of agencies to use notices to produce where the intended recipient has been notified.

3.16 The Committee acknowledges the view that when enacted the current Bill will prohibit covert access to stored communications except where an agency has a stored communications warrant.

3.17 However, the Committee also acknowledges the importance of clarifying the regime governing access to stored communications particularly for the benefit of telecommunication carriers who carry the risk of criminal and/or civil action if they disclose stored communications information in breach of the *Telecommunication Act 1997* or the *Telecommunications (Interception) Act 1979*.

Recommendation 1

3.18 The Committee recommends that the Bill be amended to include a provision amending Section 280 and subsections 282(1) and (2) of the *Telecommunications Act 1997*, effective from the same date as the Bill, to make it clear that covert access to stored communications is not permitted without a stored communications warrant.

Stored communications warrants

3.19 Under the proposed amendments a stored communications warrant will be required to access stored communications held on the carrier's equipment. The inquiry identified a number of concerns regarding the proposed warrant regime for access to stored communication, in particular:

7 Mr McDonald, *Committee Hansard*, 15 March 2006, p. 41.

- offences for which stored communications can be accessed and used; and
- enforcement agencies for which access to stored communications may be granted.

Offences for which stored communications may be accessed and used

3.20 As noted above, the proposed amendments provide an exemption to the general prohibition for stored communications accessed with a stored communications warrant. The Bill proposes two penalty thresholds that must be met in relation to accessing and the use of, stored communications. The Bill provides an initial penalty threshold that must be met for a stored communications warrant to be issued. A lower penalty threshold is then specified for the secondary use and disclosure of information which has been accessed under a stored communications warrant.

The threshold for issuing a warrant

3.21 Proposed section 116(1)(d) provides that stored communications warrants may be issued to agencies if the information likely to be obtained would assist in connection with an investigation of 'serious contraventions'.

3.22 Serious contraventions are defined at proposed section 5E as:

> (1) a contravention of a law of the Commonwealth, a State or a Territory that:
>
> (a) is a serious offence;[8] or
>
> (b) is an offence punishable:
>
> (i) by imprisonment for a period, or a maximum period, of at least 3 years; or
>
> (ii) if the offence is committed by an individual – by a fine or a maximum fine, of at least 180 penalty units; or
>
> (iii) if the offence cannot be committed by an individual – by a fine, or maximum fine, of at least 900 penalty units; or
>
> (c) would, if proved, render the person committing the contravention liable to:
>
> (i) if the contravention is committed by an individual – a pecuniary penalty, or maximum pecuniary penalty, of at least 180 penalty units; or
>
> (ii) if the contravention cannot be committed by an individual – a pecuniary penalty, or maximum pecuniary penalty, of at least 900 penalty units.

3.23 The offences for which a stored communications warrant may be issued, are significantly less than those offences for which the existing telecommunications

8 As defined in the proposed amendment to section 5D – schedule 4, item 7 of the Bill.

warrants are currently available. That is, offences punishable by imprisonment for a period, or maximum period, of at least seven years.

3.24 The Attorney-General's department advised the Committee that the distinction between real time communications and stored communications, had been recommended by the Blunn report and is based on the supposition that something that is in writing, such as emails or a text message, is 'something that definitely involves more consideration of the expression'.[9]

3.25 However, other witnesses argued that the different treatment of the two forms of communications was unjustified:

> It strikes me as nonsensical that a differentiation would be drawn between speaking to somebody on a mobile phone and sending them an SMS message. Many of the students who I teach today see them as equivalent forms of communications. It makes no sense as a matter of law or public policy why, indeed, it is easier to gain one type of information than the other … I think the proper focus for assessing this legislation is: what is the appropriate limitation upon the privacy of Australian people? For them there is no rational distinction, so I cannot see how you could justify one from the government's end.[10]

3.26 This is supported by others who argue that the proposed penalty threshold for the issuing of a stored communications warrant is too low. The Australian Privacy Foundation states:

> The principle that invasion of privacy through covert interception should only be allowed in relation to genuinely serious offences is clearly established in the existing regime. In our view, no convincing case has been mounted for why a lower threshold should apply to stored communications, which can contain information just as private, sensitive and even intimate. In the absence of any such case, it is difficult to have a rational discussion about where the threshold should be set, but we strongly urge the Committee to recommend higher thresholds than those proposed.[11]

3.27 In contrast, law enforcement agencies such as the Australian Securities and Investment Commission (ASIC) and the Australian Consumer and Competition Commission (ACCC) state that the initial three-year threshold was too high and would severely impact on the ability to carry out their legislative function. The ACCC believes that their 'ability to obtain a stored communications warrant under the Bill appears … to be quite limited.'[12]

---

9 Mr McDonald, *Committee Hansard*, 15 March 2006, p. 39.

10 Prof. Williams, *Committee Hansard*, 15 March 2006, pp 28 and 31.

11 Australian Privacy Foundation, *Submission 4*, p. 5.

12 Australian Competition and Consumer Commission, *Submission 8*, p. 6.

3.28 ASIC argued:

> The specific issue we have with the draft bill in its current form is the threshold for obtaining the warrant – three years or 180 penalty units. We have many examples of provisions throughout the Corporations Act which address serious misconduct which have a lower threshold than that. … That means that we will not be able to access that material during the course of our investigation and that will affect, to a varying degree – depending on what the information is – our investigation and our ability to assess whether or not misconduct has occurred and then our ability to take action if it has occurred.[13]

The threshold for use

3.29 The proposal in the Bill to allow for information obtained under a stored communication to be used in proceedings into offences carrying a punishment of twelve months imprisonment or sixty penalty units was supported by enforcement agencies as an appropriate threshold.[14]

3.30 However, the lower secondary threshold was strongly opposed by other organisations. EFA state that they are:

> … opposed to the provisions allowing accessed information to be disclosed and used in relation to offences and contraventions involving the much lower penalties than those for which a stored communications warrant is permitted to be used.[15]

3.31 The Attorney-General's department explained that the stored communications regime has been designed to mirror the telecommunications regime in the sense that once the higher threshold has been met for the initial privacy intrusion, the penalty for the use of that information is then dropped.

Enforcement agencies for which access may be granted

3.32 The proposed section 110 provides that an 'enforcement agency may apply to an issuing authority for a stored communications warrant in respect of a person.' The Bill inserts a new definition of enforcement agency into subsection 5(1) of the Act. It defines an enforcement agency as having the same meaning as in section 282 of the *Telecommunications Act 1997* and also includes an interception agency and eligible authority of a State.

3.33 The Explanatory Memorandum further explains that enforcement agencies 'include all the law enforcement agencies responsible for investigating criminal matters, as well as agencies responsible for administering a law imposing a pecuniary

---

13 Ms Macaulay, *Committee Hansard*, 15 March 2006, pp 16-18.

14 Australian Securities and Investment Commission, *Submission 13,* p. 2.

15 Electronic Frontiers Australia, *Submission 3,* p. 18.

penalty or administration of a law relating to the protection of public revenue.'[16] Examples of enforcement agencies include the Australian Tax Office, the Australian Securities and Investment Commission and the Australian Customs Service.

3.34 It has been argued that the range of agencies that are able to apply for stored communications warrants should be limited. The Australian Privacy Foundation considers that the extension to the breadth of access provided for in the Bill 'strikes the wrong balance between protection of privacy – the acknowledged focus of the legislation, and the exceptions for other public interests.'[17]

Committee view

3.35 The Committee acknowledges the view of law enforcement agencies relating to their requirements to access stored communications in the course of investigations related to their legislative functions.

3.36 However, the Committee notes advice from ASIC that:

> The majority of our access to emails, however, comes from access at the user's end[18]

3.37 Further the Committee notes advice that 'in the last 12 months ASIC has not accessed stored communications from an ISP.'[19]

3.38 The Committee believes that this suggests that the need for enforcement agencies to seek access to stored communications via the carrier would be limited and a general prohibition of access to stored communications would only have limited impact, if any, on the work of these agencies.

3.39 The Committee agrees that an extension of agencies for which a stored communication warrant would be available 'strikes the wrong balance' between individual privacy and effective law enforcement. The key distinction is between covert and overt searches and the principal test should be the impact on individual privacy. The Bill would result in a wide number of government agencies being able to covertly obtain material for investigating a significant range of sometimes relatively minor offences.

3.40 The Committee is of the view that the invasion of privacy resulting from covert interception of communications is significant and should therefore only be accessible to core law enforcement agencies. As well, the Committee considers that offences for which stored communications warrants may be issued should be limited to criminal offences.

---

16 Explanatory Memorandum, p. 12.

17 Australian Privacy Foundation, *Submission 4*, p. 5.

18 Mr Inman, *Committee Hansard*, 15 March 2006, p. 17.

19 Australian Securities and Investments Commission, *Submission 13A*, p. 1.

3.41 Other agencies having a legitimate need to access stored communications may continue to use the notice to produce procedures under Section 280 of the *Telecommunications Act* (as discussed above), requiring the notification of the owner of the information.

Recommendation 2

3.42 The Committee recommends that the enforcement agencies able to access stored communications should be limited to those agencies eligible under the existing arrangements for telecommunications interception.

Recommendation 3

3.43 The Committee recommends that the Bill be amended to permit stored communications warrants to be issued only in relation to criminal offences.

Required warrant information

3.44 The Bill does not require that an application for a stored communications warrant, or the warrant itself, specify either identifying information for the subject of the warrant or any specific identifying information for the telecommunications services for which the warrant will authorise access.

3.45 EFA note in their submission that 'proposed section 6EB appears to assume that a stored communications warrant would contain information identifying the person and also identifying the relevant telecommunications service … However, it is not apparent from the Bill how the issuing authority would obtain such information.'[20]

3.46 The Attorney-General's department advised the Committee that:

> The warrant would include the name of the person whom the warrant is over, including the telecommunications services that the stored communications would be attached to. All the other relevant details would be included in the affidavit. The facts and the grounds for issuing or applying for the stored communications warrant are required to be included in the affidavit.[21]

3.47 Proposed section 118 of the Bill outlines the form and content of stored communications warrants. It provides that a stored communications warrant must be in accordance with the prescribed form and may specify conditions or restrictions relating to access. Notwithstanding the advice from the Attorney-General's department, the Committee notes that subsection 118(3) only requires that:

---

20 Electronic Frontiers Australia, *Submission 3*, p. 10.

21 Ms Hume, *Committee Hansard*, 15 March 2006, p. 37.

> A stored communications warrant must set out short particulars of each serious contravention in relation to which the issuing authority issuing the warrant was satisfied, on the application for the warrant …[22]

3.48 In addition, proposed sections 111-113, which deal with the application for a stored communications warrant and the accompanying affidavit information, do not require personal or telecommunications service identification information to be provided.

Committee view

3.49 To protect the integrity of the stored communications regime and the privacy of Australians, it is essential that both the subject of the warrant and the telecommunications services for which access is sought are clearly and unmistakeably identified in the application for a stored communications warrant and on the warrant itself. The Committee notes that existing section 42(4A) currently requires such identifying information to be included in the applications for named person warrants.

3.50 The Committee notes advice that:

> … the department is currently working on the prescribed forms for which the stored communications warrants will be made.[23]

3.51 The Committee considers that given the importance of clearly identifying the subject and services for which access is sought, the requirements for such information should be settled as soon as possible for inclusion in the Bill.

Recommendation 4

3.52 The Committee recommends that the Bill be amended to require applications for stored communications warrants, and the warrant itself, to include information that clearly identifies the person who will be the subject of the warrant and the telecommunications for which access is sought.

3.53 The Committee suggests that the existing provisions for named person warrants provide a suitable example of the type of information that ought to be required.

Safeguards and privacy protection

Issuing authorities

3.54 The proposed amendments extend the range of authorities who may be declared as issuing authorities for the purposes of the stored communications warrant regime. The proposed amendments allow for stored communication warrants to be

22 Proposed subsection 118(3)

23 Mr Gifford, *Committee Hansard*, 15 March 2006, p. 37.

issued by those identified as able to issue interception warrants, 'as well as any other Commonwealth, State or Territory judge or magistrate.[24]

3.55 It has been argued that allowing AAT members to issue telecommunication interception warrants has diminished the front end accountability of Australia's interception regime.[25] The NSW Council of Civil Liberties has suggested that the increase in the number of telecommunications interceptions is a result of allowing AAT members to issue interception warrants. The Council states:

> AAT members do not have tenure, are appointed by the government and work on contract. This means that AAT members are more likely to do the government's bidding than a judge, which explains why most warrants are issued by non-judges.[26]

3.56 Evidence was provided to the Committee which stated that the proposed extension of issuing authorities for the purpose of stored communications regime will make it too easy for enforcement agencies to obtain a warrant. The Australian Privacy Foundation argued:

> Restricting warrant issuing authority to judges, full time federal magistrates and full-time senior AAT members would be an important safeguard against it becoming too easy to for [sic] enforcement agencies to obtain a warrant.[27]

3.57 The Attorney-General's department explained the proposal to increase the range of issuing authorities as:

> … trying to get a balance. As ASIC said earlier, 'We don't see why these electronic things should be treated any different to any other hard copy document.' So you have that angle to it. Of course, a search warrant can be issued by a magistrate … I think Tony Blunn in his report makes this point that there is a distinction between something that is live and something that is being composed and stored like a document. Consequently, because of those factors, Mr Blunn recommended that it was appropriate to have it as a magistrate.[28]

Committee view

3.58 As discussed above, the Committee rejects the proposition that stored communications are equivalent to normal search warrants. The key differentiating factor is the covert nature of the stored communication warrant. For this reason, the

---

24 Explanatory Memorandum, p. 12.

25 Bronitt, S. and Stellios, J., Telecommunications interception in Australia: Recent trends and regulatory prospects, *Telecommunications Policy 29 (2005),* p. 886.

26 NSW Council of Civil Liberties, 'Australian phones 26 – times more likely to be bugged than an American phone', *Media Release,* 13 January 2006.

27 Australian Privacy Foundation, *Submission 4,* p. 4.

28 Mr McDonald, *Committee Hansard,* 15 March 2006, p. 39.

Committee does not accept that stored communications should be afforded any less privacy than is afforded to real time communications.

3.59 As such, the Committee does not consider a comparison between stored communications and hard copy documents justifies an extension of the issuing authorities to include magistrates. It is also noted that no evidence has been produced to suggest that the current arrangements are inadequate. In practice, an increase in the number of issuing authorities seems likely to make stored communications warrants more readily available.

Recommendation 5

3.60 The Committee recommends that the Bill be amended to allow issuing authorities to only include those currently able to issue interception warrants.

Enforceability in relation to State/Territory agencies

3.61 EFA highlight in their submission that while the Bill intends to regulate access to, and the use of, stored communications it is not clear if the Commonwealth would have the ability to enforce the provisions proposed in the Bill. According to EFA:

> In the case of interception information, this issue is dealt with by the legislated requirement that State and Territory Parliaments enact complementary interception legislation applicable to their agencies and responsible Minister prior to the (C'th) Minister being permitted to declare such agencies as 'eligible' interception agencies … However, there is no indication in either the Bill or Explanatory Memorandum of any intent to require State/Territory Parliaments to amend their interception legislation to complement the Commonwealth provisions concerning use, communication and recording of information obtained by accessing stored communications, and related reporting requirements.[29]

3.62 EFA advised the Committee that the issue would be remedied by requiring, as a precondition to being granted the powers of an enforcement agency under the stored communications regime, State and Territory Parliaments to enact complementary legislation. Given the tight timeframe for the implementation of such measures, as an additional safeguard EFA suggests that the Minister could be given the power to 'remove from state or territory agencies the right to get a warrant under the Commonwealth Telecommunications (Interception) Act.'[30]

3.63 This would provide similar protections as those provided by existing section 34 for telecommunications interception which allows the Minister, 'by legislative instrument and at the request of the Premier of a State, declare an eligible authority of that State to be an agency for the purposes of this Act' subject to certain conditions.

---

29 Electronic Frontiers Australia, *Submission* 3, pp 16-17.

30 Ms Graham, *Committee Hansard*, 15 March 2006, p. 14.

Committee view

3.64 The Committee considers it essential that the Commonwealth has the ability to enforce the obligations prescribed in the Bill relating to accessing stored communications. Immediate action should be taken to ensure enforceability of these provisions on State and Territory agencies.

3.65 The Committee considers that consistent with the arrangement for the existing telecommunications interception regime, State and Territory Parliaments should be required to enact complementary legislation for access to stored communications as a precondition to being granted the powers of an enforcement agency under the stored communications regime.

3.66 In light of the tight timeframe, the Committee supports the idea of amending the Bill to enable the exclusion of particular State/Territory agencies as an interim measure.

Recommendation 6

3.67 The Committee recommends that, consistent with the existing arrangements for telecommunications interception, immediate action be taken to ensure the enforceability of the stored communications provisions on State and Territory agencies by requiring complementary legislation to be enacted as a precondition to being granted the powers of an enforcement agency under the stored communications regime.

Recommendation 7

3.68 The Committee also recommends that as an interim measure, the definition of an enforcement agency in the Bill be amended to allow for the ability to exclude an agency specified in the Telecommunications Interception Regulations from being able to obtain a stored communications warrant.

Matters which issuing authorities must consider

3.69 The Bill proposes at section 116(2) that issuing authorities must have regard to:

(a) how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant; and

(b) the gravity of the conduct constituting the serious contravention; and

(c) how much the information referred to in paragraph (1)(d) would be likely to assist in connection with the investigation; and

(d) to what extent methods of investigating the serious contravention that do not involve the use of a stored communications warrant in relation to the person have been used by, or are available to, the agency; and

(e) how much the use of such methods would be likely to assist in connection with investigation by the agency of the serious contravention; and

(f) how much the use of such methods would be likely to prejudice the investigation by the agency of the serious contravention, whether because of delay or for any other reason.

3.70 The proposed approach is generally supported. However, it is suggested that that the issuing authority should be permitted to take additional considerations into account such as length of time stored communications have been stored and whether a search can be undertaken to obtain the relevant information.[31] Further, whether or not the stored communications are likely to include communications the subject of legal professional privilege and whether such communications should be placed in confidential safekeeping of an independent person should also be considered.[32]

Committee view

3.71 The Committee is of the view that individual privacy protection ought to be the chief consideration in any regime permitting access to personal communications. This is particularly important where communications may include information subject to legal professional privilege. The Committee considers that additional considerations for issuing authorities such as those suggested above will only serve to enhance the privacy protection already outlined in the Bill.

Recommendation 8

3.72 The Committee recommends that the Bill be amended to allow issuers of stored communications warrants to have regard to the length of time stored communications may have been held on a carrier's equipment and whether the communications sought can be sufficiently identified in order to minimise the impact on privacy.

Recommendation 9

3.73 The Committee also recommends that the Bill be amended to require issuers of stored communications warrants to consider whether the stored communications are likely to include communications the subject of legal professional privilege and whether any conditions may be implemented to prevent the disclosure of such communications.

Destruction of irrelevant information

3.74 Access to stored communications, by its very nature, results in the increased likelihood of the collection of large amounts of information that may not be relevant to the investigation for which the warrant was issued. Therefore, adequate provisions governing the destruction of irrelevant material are a vital privacy safeguard.

---

31 Electronic Frontiers Australia, *Submission* 3, pp 13-14.

32 Electronic Frontiers Australia, *Submission* 3, pp 13-14.

3.75 Proposed section 150 provides for the destruction of records obtained by accessing a stored communication. Specifically it states that:

> if the chief officer of the agency is satisfied that the information or record is not likely to be required for a purpose referred to in subsection 139(2); the chief officer must cause the information or record to be destroyed forthwith.[33]

3.76 In their submission, the Office of the Privacy Commissioner suggested that the effect of proposed section 150 may result in it being 'lawful for an agency to keep irrelevant information indefinitely.'[34] This is due to the fact that an obligation to destroy irrelevant information does not arise until after the chief officer has formed a view that the information is no longer required without the Bill specifying a time limit for this to occur.

3.77 The Office of the Privacy Commissioner recommended that, consistent with good privacy practice:

> consideration be given to amending the Bill to ensure that agencies take regular steps to review whether information they have accessed via stored communications warrants is still required for a permitted purpose eg; by setting a maximum period for review.[35]

3.78 The Attorney General's department argued it did not expect that any law enforcement agency that is permitted to access stored communications would fail to assess irrelevant information on a regular basis. As well, they advised the Committee that 'there is also the additional safeguard that there is a prohibition on the use of any information.'[36]

Committee view

3.79 The Committee considers that setting a maximum period for review of information obtained via a stored communications warrant will require agencies to establish procedures to deal with irrelevant information in a timely manner. Given the potential to collect vast amounts of irrelevant information under a stored communications warrant the Committee believes that such a safeguard is essential.

3.80 The Committee notes the assurances of the Attorney-General's department that the relevance of collected information would be considered in a timely manner, however these are not requirements that are contained in law. The legislation must also guard against any lapses in administrative practices within agencies. Furthermore, the Committee considers that such a requirement is particularly important given the

---

33 Proposed section 150(1)(b)

34 Office of the Privacy Commissioner, *Submission 6*, p. 2.

35 Office of the Privacy Commissioner, *Submission 6*, p. 2.

36 Mr Gifford, *Committee Hansard*, 15 March 2006, p. 42.

proposal in the Bill to extend the access to stored communications to a range of agencies that are not used to dealing with intercepted material as a matter of course.[37]

Recommendation 10

3.81 The Committee recommends that the Bill be amended to specify time limits within which an agency must both review their holdings of information accessed via a stored communications warrant and destroy information as required under the proposed section 150.

Monitoring of the stored communications warrant regime

Proposed reporting requirements

3.82 The Bill proposes lower reporting requirements for the use and effectiveness of stored communications warrants in comparison to the existing telecommunication interception warrants. The Explanatory Memorandum states that the reporting requirements for stored communications warrants are not as burdensome on the agencies as the reporting requirements for interception and these are consistent with general search warrant provisions and reflect the lower threshold to be met.[38]

3.83 However, the primary consideration of a regime which permits access to personal communications ought to be the protection of privacy. Stored communications warrants can not be considered the equivalent of search warrants due to their covert nature.

3.84 In their submission, EFA argues:

> Reporting obligations are necessary due to the covert and secretive nature of warrants and resultant potential for abuse. The fact that warrants will be available in relation to contraventions involving lesser penalties increases, not decreases, the potential for abuse.[39]

Role of the Ombudsman

3.85 The proposed amendments expand the functions of the Ombudsman considerably to include oversight of the stored communications regime. Section 152 proposes additional functions including:

> (a) to inspect an enforcement agency's records in order to ascertain, so far as is practicable, the extent of compliance, in relation to those records with sections 150 and 151; and
>
> (b) to report to the Minister about the results of inspections under this Division; and

37 Senator Payne, *Committee Hansard,* 15 March 2006, p. 42.

38 Explanatory Memorandum, p. 13.

39 Electronic Frontiers Australia, *Submission 3,* p. 19.

(c) to do anything incidental or conducive to the performance of any of the preceding functions.

3.86 In his submission the Ombudsman advised the Committee that:

> Whether my office is able to inspect most, if not all, agencies, in the spirit of the proposed amendments, or whether we will be able to inspect only a few, will depend on whether additional resources are available.[40]

3.87 The Ombudsman also advised the Committee that if a considerable number of enforcement agencies were inspected, the reporting timeframes may be difficult to meet. The Ombudsman went on to suggest:

> It would be preferred if the proposed reporting timeframes for section 153 reports could be extended to six months instead of three. This should not interfere unduly with the accountability objective while allowing more time for reports to be prepared that are as useful and comprehensive as they can be.[41]

Committee view

3.88 The Committee agrees with the view that reporting obligations are vital to provide adequate transparency and accountability for the stored communications warrant regime. The Committee agrees with the position that a lower offence threshold does not equate to a lesser reporting obligation.

3.89 As well, the Committee considers that the Ombudsman will undertake a vital role in the oversight and inspection of the stored communication regime. The Committee acknowledges the view expressed by the Ombudsman with regard to the impact that resources will have on his ability to fulfil the additional functions required under the Bill. The Committee is of the view that limited resources should not prevent adequate oversight of this regime. Therefore, the Committee considers that the Government should review the funding levels of the Commonwealth Ombudsman to provide the requisite additional resources to adequately fulfil this expanded function.

3.90 The Committee also supports allowing an additional three months to enable the production of useful and comprehensive reports.

Recommendation 11

3.91 The Committee recommends that Bill be amended to require agencies and the Minister to report on the use and effectiveness of stored communications warrants in a manner equivalent to the existing reporting obligations for telecommunications interception warrants.

---

40 Commonwealth Ombudsman, *Submission 10*, p. 2.

41 Commonwealth Ombudsman, *Submission 10*, p. 3.

Recommendation 12

3.92 The Committee recommends that additional resources be provided to the Ombudsman to enable the Office to fulfil the expanded functions under this Bill.

Recommendation 13

3.93 The Committee recommends that the Bill be amended to extend the timeframe for section 153 reports to six months.

Stored Communications and related definitions

3.94 The Bill inserts new definitions into the Act to support the establishment of the stored communications access regime.

3.95 Stored Communications is defined by the Bill as:

> … a communication that:
>
> (i) has passed over a telecommunications system; and
>
> (ii) is not passing over a telecommunications system; and
>
> (iii) is held on equipment that is operated by, and is in the possession of, a carrier; and
>
> (iv) is accessible to the intended recipient of the communication.

Copies of stored communications

3.96 In relation to the definition of stored communications as proposed in the Bill, EFA argues:

> In our view the definition results in insufficient clarity and certainty in relation to some types of records of communications held on carriers' equipment. For example, it is not clear whether a **copy** of a stored communication that is stored on a carriers' equipment, but is **not** accessible to the intended recipient of the communication, is to be regarded as a 'stored communication' or not.[42]

3.97 EFA suggest that copies of communications stored in a sender's sent box on a carrier's equipment, or communications stored on a carrier's backup device are examples of communications which may be regarded as copies of communications rather than stored communications.

3.98 The Attorney-General's department advised:

> A copy of a stored communication accessed by the person on the premises – so any end point of the communication – will not require a stored communications warrant. It is only those communications which are

42 Electronic Frontiers Australia, *Submission 3,* p. 6.

> accessed directly from the carrier which will require a stored communications warrant.[43]

Definition of accessing a stored communication

3.99 In their submission, EFA highlight that accessing a stored communication as provided for in section 6 of the Act refers to among other things, 'recording such a communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication.'[44]

3.100 However, recording a communication, as defined in the Act, does not specifically address recording in relation to accessing a stored communication.

3.101 EFA suggest that:

> The definition of a record should be amended so that it applies in relation to, not only an interception, but also accessing a stored communication.[45]

Access to stored communications via the sender

3.102 In regard to the definition of stored communications, Telstra advised that it appears to limit stored communication warrants to accessing communications **received** by a person of interest, but not those communications **sent** by the person of interest. Telstra stated that:

> Carriers cannot necessarily know whether, or when, a communication that has been sent has been received by the intended recipient and, therefore, whether a communication that has been sent has become a stored communication. As such, communications that have been received by a person of interest would be stored communications, and could be accessed under a stored communications warrant. In contrast, communications that have been sent by the person of interest would not be stored communications, and therefore, could not be accessed under a stored communications warrant.[46]

3.103 The Attorney-General's department advised the Committee that:

> That question, of whether or not access is available via the sender, is still under active consideration by the government in terms of making sure it makes sufficient allowance for our operational needs.[47]

---

43 Mr Gifford, *Committee Hansard,* 15 March 2006, p. 36.

44 Proposed section 6AA

45 Electronic Frontiers Australia, *Submission 3,* p. 8.

46 Telstra, *Submission 20,* p. 2

47 Mr Gifford, *Committee Hansard,* 15 March 2006.

Unsolicited commercial electronic messages

3.104 In their submission, the Australian Communications and Media Authority (ACMA) highlight that as currently drafted the definition of stored communications would adversely impact the ACMA's ability to enforce the *Spam Act 2003* (the Spam Act). ACMA state that:

> … any spam message that falls outside the definition of a stored communication will not be accessible by ACMA investigators under the proposed warrant regime and would therefore be unavailable to ACMA investigators in their enforcement of the Spam Act.[48]

3.105 The Attorney-General's department advised the Committee that:

> This is an issue that ACMA has raised with us previously. It is a matter on which we continue to work collaboratively with ACMA and the Attorney is well versed on this particular issue.[49]

3.106 The Committee is of the view that it is essential that the definitions proposed in the Bill provide sufficient clarity to support the effective operation of the stored communications warrant regime. The Committee acknowledges the advice from the Attorney-General's department that in some cases work is continuing. However, the Committee considers that definitional issues should be settled prior to the passage of the Bill.

Recommendation 14

3.107 The Committee recommends that the Bill be amended to ensure that copies of communications can not be accessed without a stored communications warrant.

Recommendation 15

3.108 The Committee recommends that the definition of 'record' be amended so that it applies in relation to accessing a stored communication.

Recommendation 16

3.109 The Committee recommends that the issue regarding whether or not access to stored communications is accessible via the sender is settled and the Bill be amended as necessary.

Recommendation 17

3.110 The Committee recommends that prior to the passage of the Bill the definition of stored communications be amended so that the Australian

48 Australian Communications and Media Authority, *Submission 18*, p. 2.

49 Mr Gifford, *Committee Hansard*, 15 March 2006, p. 34.

Communications and Media Authority's ability to enforce the Spam Act is not limited.

Peer-to-peer networks

3.111 The proposed definition of stored communication provides that a stored communication is defined to mean a communication that, among other things, is held on equipment operated by the carrier at its premises. The Explanatory Memorandum states that:

> This is to ensure that … the stored communications regime only applies to accessing stored communications via a telecommunications carrier. The regime does not affect existing lawful access to communications stored on a person's telecommunication device.

3.112 Communications are not considered 'stored communications' if they are unable to be accessed via the carrier. However, current technology allows individuals to share content files[50] via the peer-to-peer model (file sharing). The peer-to-peer model allows files to be stored on and served by personal computers of the users. Pure peer-to-peer networks do not have a central server managing the network or a central router.

3.113 Since the stored communications regime applies only to communications held by a telecommunications carrier, it will not extend to allow access to other communications and information shared via a peer-to-peer network. This may therefore, allow persons of interest to avoid covert access to their stored communications by law enforcement agencies.

3.114 The intent of the Bill has been described as assisting 'law enforcement and security agencies to keep pace with increasingly sophisticated methods of avoiding detection.'[51] The Committee acknowledges the challenges associated with developing technology neutral interception and access regimes, particularly given rapid technological advances. However, increased use of peer-to-peer technology is likely to have a considerable impact on the effectiveness of the stored communications regime proposed in the Bill.

---

50 Content files can contain audio, video, data or anything in digital formal, as well as real-time data, such as Voice over Internet Protocol.

51 Ruddock, P., *Interception amendments achieve appropriate balance*, Media Release, 16 February 2006.

CHAPTER 4

B-PARTY INTERCEPTION

Introduction

4.1 One of the most contentious aspects of the Bill is contained in Schedule 2 which deals with the so-called 'B-party' warrants. Briefly, in the words of the Explanatory Memorandum, the provisions 'enable interception of communications of a person known to communicate with the person of interest'.[1]

4.2 B-party warrants are issued by the Attorney-General in the case of an application by the Director-General of ASIO, or by an 'eligible judge' or member of the AAT in the case of an application by a law enforcement agency.

4.3 The warrant may only be issued for offences which attract a maximum penalty of seven years' gaol. Further, they will only be issued to an interception agency which has satisfied the issuing authority:

- that it has exhausted all other methods of identifying a telecommunications service used by a person of interest; or that it is not possible to intercept the communications of the person of interest; and
- that the person being intercepted will likely be contacted by the person of interest on the service being intercepted.

4.4 When issuing the warrant, the issuing authority must also have regard to the following:

- the extent to which the proposed interception interferes with the privacy of any person;
- the gravity of the offences being investigated;
- the extent to which the information obtained under the warrant will assist the investigation;
- the extent to which alternative methods of investigation have been used or are available to the agency; and
- the extent to which these alternative methods would be useful to or would prejudice the investigation.

---

1 Explanatory Memorandum to the Telecommunications (Interception) Amendment Bill 2006, p. 1.

4.5 Once issued, the warrants are available for 45 days for law enforcement agencies and 30 days for ASIO. This is half the time provided for the execution of existing telecommunications interception warrants.

Rationale for B-party interception warrants

4.6 The necessity for this type of interception warrant was explained by the Attorney-General in his Second Reading speech. The Attorney General said:

> This amendment will assist interception agencies to counter measures adopted by persons of interest to evade telecommunications interception, such as adopting multiple telecommunications services. The ability, as a last resort, to intercept the communications of an associate of a person of interest will ensure that the utility of interception is not undermined by evasive techniques adopted by suspects.

4.7 The provisions had their genesis in the *Report of the Review of the Regulation of Access to Communications* ('The Blunn Report').2 In Part 12 of that report, Blunn observed that the current *Telecommunications Interception Act 1979* does not authorise the use of B-Party intercepts.[3]

4.8 In his exploration of the issue, Blunn observed that the security and law enforcement agencies argue that there is a need for B party interception, and noted its usefulness in appropriate circumstances. However he cautioned the need for 'appropriate controls, and the need to acknowledge and deal with the significant privacy implications.'4 Accordingly, his Recommendation 12 states:

> I recommend that the Interception Act be amended to make it clear that B-Party services may be intercepted in limited and controlled circumstances.[5]

4.9 Officers of the Attorney-General's Department gave more detailed evidence of this issue to the Committee. Mr Geoff McDonald Assistant Secretary of the Security Law Branch explained that:

> … we are facing a practical problem which some law enforcement agencies are very concerned about. It is due to people becoming more savvy about these matters. ... People are savvy enough now, if they are involved in the criminal side of things, to use the technology.[6]

4.10 From a policing point of view, the Deputy Commissioner of the Australian Federal Police observed that the proposals would clarify the position in relation to

---

2 Blunn, A S, AGPS, August 2005

3 Blunn, p. 76.

4 Blunn, p. 76.

5 Blunn, p. 77.

6 *Committee Hansard*, 15 March 2006, p. 52.

B-party warrants and provide an 'important investigative tool' for the AFP.[7] He explained:

> Where we have … multiple phones changing and SIM cards changing, it is often hard for law enforcement to identify the suspect's telecommunications service. Intercepting a close or known associate, somebody who we have to satisfy in accordance with the criteria you have just heard about and in the context of an affidavit before a magistrate as to what the nexus between the two is and why we believe that may produce the communications service of the suspect, is necessary.[8]

4.11 Assistant Commissioner Lawler gave several examples of situations in which the amendments would assist police. He proffered the following hypothetical case:

> With suspected purchases of explosive chemicals that are outside the norm, a particular chemical company has come forward and advised us that a particular person will call in. He does not know who the person is. He might have given a name; it could be false, but they will ring in to the chemical company and advise delivery and other sorts of details et cetera. The B-party warrant in that situation, given the current legislation, says that the person must be involved in the offence. [9]

4.12 In another example, he explained that:

> … when we use undercover operatives or cooperating informants it is often necessary to have these people call particular individuals to gather evidence as to the ongoing commission of offences or offences that may have been perpetrated. That is one of the tactical techniques but as it currently stands under the law one cannot get a telephone intercept because one is required to establish that the service belongs to a person who is involved.[10]

4.13 The Committee also notes that an important element of the current proposal is the clarification of the existing law on B-party warrants, which appears to give partial approval for their use.

4.14 As Mr Blunn commented, this matter was explored by the Federal Court in *John Flanagan and Ors v the Commissioner of the AFP and ors FCA (1995)* in which the court upheld the validity of B-party interception under the existing interception warrant regime but 'did not provide any useful analysis of the rationale'.[11] Assistant Commissioner Lawler indicated that the case created ambiguity and uncertainty over lawfulness of B-party interception under the Section 45 and 45A provisions:[12]

---

7 *Committee Hansard*, 15 March 2006, p. 32.

8 *Committee Hansard*, 15 March 2006, p. 44.

9 *Committee Hansard*, 15 March 2006, p. 46.

10 *Committee Hansard*, 15 March 2006, p.

11 Blunn, p. 76.

12 *Committee Hansard*, 15 March 2006, p. 45.

> … there are examples where some of the circumstances surrounding the current legislative provisions, namely, 45 and 45A, actually capture the spirit of B-party warrants.[13]

4.15 Mr Geoff McDonald of the Attorney-General's Department expanded on this:

> The interesting thing about it is that it can so easily be restricted to the facts of a particular case and distinguished, but from a policy perspective we certainly need to have a decent codified position on this rather than trying to rely on peculiar facts of a particular case.[14]

4.16 The Committee notes that in his submission to the Committee, the Hon Duncan Kerr SC MP refutes the existence of any common-law right for third party interception, and states that the only lawful basis for the interception of a telephone service is through the *Telephone (Interception) Act 1979*.[15]

4.17 The Committee further notes the statement of Mr Carnell, Inspector General of Intelligence and Security:

> the nature of B-Party interception warrants inherently involves a potential for greater privacy intrusion for persons who may not be involved in activities of legitimate concern under the ASIO Act. As a result, particular attention will be given to the additional legislative tests for this type of warrant, as well as checking that the duration of 90 days is adhered to.[16]

The counter view: B-party interception not necessary

4.18 Other submissions rejected outright these justifications for the creation of the warrants, arguing that they are an unwarranted invasion of privacy and that the necessary information can be gained by existing means.

4.19 Mr Cameron Murphy of the NSW Council for Civil Liberties, while acknowledging that the purpose of the principal Act is to protect the privacy of people using communications devices, remained concerned that this amendment represents 'a massive expansion of the invasion into people's privacy who use telecommunications devices' and maintained that there is no real justification for it:

> We can accept that, if someone is a suspect in a criminal investigation, it is a matter of balancing the interests of the public in ensuring that that suspected offence is investigated and that the person is prosecuted and dealt with under the law. In this amendment, we are dealing with something that goes much further than that. We are talking about innocent B-parties, people who are not themselves suspected of any offence … B-party warrants … shift[s] the focus of the investigation from someone who is a

13 *Committee Hansard*, 15 March 2006, p. 44.

14 Ibid.

15 *Submission* 1, p. 4.

16 Submission 9, pp 2-3.

> suspect to an investigation surrounding the innocent B-party on the off-chance that a suspect might contact them and there might be useful information gleaned that way…. [17]

4.20 Similarly, the Law Council of Australia observed that:

> Schedule 2 of the Bill if enacted allows certain law enforcement agencies and ASIO to intercept telecommunications of a person who has no knowledge or involvement in a crime, but who may be in contact with someone who does. In other words, people suspected of nothing will be under surveillance. … This is the first time ever in Australia's history that law enforcement agencies will be given power to intercept telecommunications of people who are not suspects, who are innocent people.[18]

4.21 In their submission to the inquiry, the Gilbert and Tobin Centre of Public Law states:

> We believe, however, that the Bill abrogates the right to privacy substantially more than is necessary to achieve the Bill's security purposes. It is important that legislation does not abrogate rights more than is necessary and incidental to achieving the purpose of the legislation.
>
> Where legislation does disproportionately abrogate rights, it may have adverse, unintended effects.[19]

4.22 Electronic Frontiers Australia was also concerned about the provisions, the Executive Director saying that the organisation is 'completely opposed' to the B-party warrant provisions. Similarly, the Australian Privacy Foundation urges the provisions be excised from the Bill until they can be given further consideration.[20]

4.23 The Law Council of Australia argued that the proposals breach Article 17 of the International Covenant on Civil and Political Rights and described the proposals as an 'arbitrary' invasion of privacy.[21]

4.24 The NSW Council for Civil Liberties agreed and further said that the provisions are also unjustified on practical grounds. Mr Murphy told the Committee:

---

17 Ibid.

18 *Submission* 17, p. 6.

19 *Submission* 2, p. 1.

20 *Submission* 4, pp 8-9.

21 *Committee Hansard,* 15 March 2006, p. 2, Submission 17, p. 6.

Article 17 ICCPR states:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

> It appears to us that any of the evidence sought by law enforcement agencies could be obtained through an ordinary service warrant or a named person warrant. We have not yet seen a single example that stands up to even basic scrutiny about why a B-party warrant might be needed in order to obtain evidence about the suspect.[22]

Committee view

4.25 The Committee accepts that rapidly developing technology, and the increasing tactical sophistication of the targets of investigations, requires new approaches by law enforcement agencies if they are to remain effective. The current uncertainty of the law relating to B-party interception also requires clarification, both for law enforcement agencies and to ensure the proper protection of privacy. For the Police and the Department, the legislation represents a codification, and clarification of a situation which arguably exists at present.

4.26 The Committee notes that in many cases, those who expressed reservations about B-party warrants acknowledged that in very rare circumstances there may be some justification for them. Mr Timothy Pilgrim, Deputy Privacy Commissioner summarised the resulting dilemma:

> … we also recognise that the community expects that law enforcement agencies will have access to appropriate tools to allow them to efficiently undertake one of their key roles in the community – that of investigating criminal activities. The challenge facing the community is where to strike the right balance between these important community priorities. Is the response, for example, proportional to the risk that has been identified?[23]

4.27 Similarly, the Committee accepts the need for B-party warrants. However, the invasion of privacy of innocent parties who become the subject of surveillance merely by reason of association is very significant. The key question is therefore the extent to which the Bill provides a framework of controls over the proposed warrants to balance privacy protection with effective law enforcement.

4.28 Evidence from witnesses and submissions perceived various shortcomings and ambiguities in the B-party warrant provisions. In particular, concerns focused on:

- the differences in the thresholds for issuing B-party interception warrants and others under the legislation;
- controls on the dissemination of information beyond the B-party, and the possible derivative use of information obtained under the warrant;
- the implications for the protection of privileged communications;
- reporting and accountability requirements; and

22 *Committee Hansard*, 15 March 2006, p. 56.

23 *Committee Hansard*, 15 March 2006, p. 22.

- the need for a review of the legislation.

4.29 These issues are considered below.

Issuing B-party interception warrants

4.30 The Bill proposes two separate regimes for issuing B-party warrants: one for ASIO on application by the Director-General of Security, and another for law enforcement agencies. Evidence to the inquiry argued that the parameters for the issuance of these warrants is too wide.

Applications by the Director-General of Security

4.31 Under this proposal, B-party interception warrants could be issued to ASIO by the Attorney General (proposed Subsection 9(3)). Two issues emerged in relation to this.

4.32 The first relates to the proposed issuing authority. The Law Council was of the view that these warrants should be the subject of judicial oversight rather than being issued by a member of the executive; the council considers this is the best approach where decisions erode fundamental human rights such as interference with a person's liberty such as the unlawful interference with a person's right to privacy.[24]

4.33 In response, Mr McDonald explained that the Attorney-General has been always had responsibility for issuing telecommunications warrants, to ASIO and the safeguards which apply to other warrants issued by the Attorney will also apply to B-party warrants.[25]

4.34 The Committee notes that this measure is consistent with similar warrant regimes in the legislation; however the Committee also emphasises that these warrants are not the same as the existing TI warrants, which deal directly with persons of interest; they are third party warrants, targeted at people who may have only a very tenuous link with the person of interest.

4.35 At the same time, the Law Council's desire for judicial consideration of warrant applications appears to promote a visibly more independent approach to the issue of security warrants, although the Committee notes that in issuing a TI warrant a judge is not making a judicial decision but an administrative one.

4.36 The second matter relates to the threshold criteria for issuing the warrant. Professor Williams noted in his submission that under Item 1 of Schedule 2:

> … there is no requirement that there be evidence of a nexus between B-Party communications and the activities prejudicial to national security which triggered the warrant. All that must be shown is that: (i) the B-Party

24 *Submission* 17, p. 9.

25 *Committee Hansard*, 15 March 2006, p. 50.

> is likely to communicate with a person who is likely to engage in activities prejudicial to security; and (ii) intercepting the B-Party's communications is likely to assist in obtaining intelligence related to security.[26]

4.37 Professor Williams observes that the purpose of B-party interceptions is to assist investigations of matters prejudicial to security.[27] However, he considers the Bill grants far more extensive powers than necessary to achieve this. They may be issued in the absence of any evidence that the warrant will contribute to information about the activities which give rise to the warrant. He continued:

> It is enough to show that intercepting B-Party communications to or from *anyone* may assist in obtaining *any* intelligence related to security.[28]

4.38 Further, Professor Williams notes that the application by the Director-General must only show that the interception would be 'likely to assist' in obtaining intelligence related to security; according to Professor Williams both the terms 'likely to assist' and relating to security' are wide and vague.

4.39 The resulting powers potentially allow ASIO to engage in the kind of 'fishing expeditions' of which the Blunn report warned.[29] The B-party warrants have the potential to obtain online information on a continuous basis, allowing tracking of persons via a telecommunications device, or simply the gleaning of general information about a person's associates. If this use is intended then there should be explicit reference to it in the legislation. This breadth and vagueness could create the potential for abuse of the interception power.

4.40 Professor Williams suggested that the Bill be amended to provide for a precondition in section 9 to issuing a warrant. This would require evidence that the B-party's telecommunications service is likely to be used to communicate or receive information relevant to the particular activities prejudicial to security which triggered the warrant.

4.41 The Committee considers that this provision is far too vague. The proposal involves access to material generated by innocent persons, and must be circumscribed as far as possible to protect their privacy. The Committee notes that in comparison, search warrant regimes require applicants to establish a connection between the item sought and the offence being investigated – not to matters which are 'likely to assist'. There appears no reason why the conditions applying to warrants sought by the Director-General should not also contain analogous conditions to avoid the kind of 'fishing expedition' of concern both to Blunn and the Centre for Public Law.

4.42 Accordingly the Committee recommends:

---

26 *Submission* 2, p. 2.

27 Ibid

28 Ibid

29 Blunn, p. 74.

Recommendation 18

4.43 The Committee recommends that as a precondition to issuing a warrant under subsection 9(3), there must be evidence that the B-party's telecommunications service is likely to be used to communicate or receive information relevant to the particular activities prejudicial to security which triggered the warrant.

Applications by law enforcement agencies

4.44 Submissions to the Committee generally sought more stringent requirements for demonstrating the necessity for the B-party warrant. Electronic Frontiers Australia's submission states:

> It should be required that any agency requesting such a warrant establish to the satisfaction of the issuing authority evidence to support their belief that the information likely to be obtained from the interception is material to the investigation and that such information cannot be obtained by any means other than by interception of a B-Party telecommunications service.[30]

4.45 EFA also suggested that agencies should have to provide evidence about the type of service – business, private, high or low volume – so as to give the issuing authority relevant information to be considered when assessing the extent of the invasion of privacy of innocent party communications that is proposed. This includes not only the innocent B-party, but other innocent persons with whom the B party communicates.

4.46 Similar to EFA's first proposal, Professor Williams observed:

> Under items 8 and 9 of Schedule 2 (amending s 46), the issuing officer must be satisfied that the warrant will assist in obtaining evidence relating to the offence which is being investigated before a warrant may be issued.
>
> … These items do not, however, require that it be established that the evidence will be obtained from communications between the B-Party and the person suspected of being involved in the offence. It would be sufficient, for instance, if: (i) the B-Party sometimes communicated with the suspect; and (ii) intercepting communications between the B-Party and any third party would, in some way, assist in investigating the suspect. This is a particularly low burden.[31]

4.47 Professor Williams suggested that the preconditions for issuing a warrant under section 46 should include evidence that the 'suspect will, in some way, be causally related to communications involving the B-party which will assist in investigating the suspect.'

---

30 *Submission 3*, pp 28-29.

31 *Submission 2*, p. 3.

4.48 The Blunn report suggested that appropriate control requirements might provide that:

> … any agency requesting such a [B-party] warrant must establish to the satisfaction of the issuing authority evidence to support their belief that the information likely to be obtained from the intercept is material to the investigation. The agency should also establish that it cannot be obtained other than by telecommunications interception or the use of a listening device. It is then for the issuing authority to consider that evidence along with any other relevant matters such as the invasion of privacy involved and the gravity of the alleged offence in deciding whether to issue a warrant.[32]

4.49 When this matter was raised with the officers of the Attorney-General's Department, the Committee was advised that 'a lot of the safeguards that apply to TI more generally apply to B-party'.[33] However it emerged in discussions that the suggestion of Mr Blunn had not been taken up in drafting the bill, and that the only additional requirement applying to B-party warrants other than the general conditions was a requirement that:

> … the agency must demonstrate that it has exhausted all other practical methods of identifying the telecommunications service to be used or likely to be used by the suspect or that it is not possible to actually intercept the service being used by the suspect. That is to ensure that it is a measure of last resort and that it is done in those circumstances which are operationally required.[34]

4.50 The Committee notes that notwithstanding both the Attorney General's and the department's use of the expression 'last resort', the term does not appear in the bill, although the phrase in Schedule 2 of the bill refers to having 'exhausted all other practicable methods'.[35] Whether or not the conditions truly represent a last resort was a matter of some contention. The Law Council suggested that:

> … for the measure to be applied as a last resort, the agency should have exhausted all other means of surveillance and tracking of the suspect and not merely exhausted all other practicable methods pertaining to telecommunications services used or likely to be used by the suspect.[36]

4.51 The Council for Civil Liberties was also of the view that the process as described did not amount to a 'last resort', nor is it clear what the exhausted 'practical means' may be. Mr Murphy pointed out that this could well refer to economic efficiency or convenience.[37]

---

32 Blunn, p. 77.

33 *Committee Hansard*, 15 March 2006, p. 43.

34 Mr Gifford, *Committee Hansard*, 15 March 2006, p. 44.

35 *Committee Hansard*, 15 March 2006 p. 47.

36 *Submission* 17, p. 9.

37 *Committee Hansard*, 15 March 2006, p. 59.

Consenting to telecommunications intercepts

4.52 It was confirmed by the AFP at the hearing that the current TI arrangements do not provide for a situation where a person could consent to an intercept being placed on their service.[38] Neither is it contemplated under the current Bill.

4.53 This is not a matter that the Committee has had time to consider in adequate detail to form any conclusions. However, given the seriousness privacy implications of the B-party warrants, it is an area that deserves further consideration.

Committee view

4.54 The Committee notes that the B-party warrant is a particularly invasive tool for the detection of criminal activity. As previously acknowledged such tools may be necessary in some circumstances, but the basis for authorising them must take account of their unique nature. A B-party warrant applied to a non-suspect is simply not the same as the current regime of telephone intercept warrants applied to those suspected of serious criminal offences. The *Telecommunications (Interception) Act 1979* prescribes very closely the circumstances in which telecommunications can be intercepted, surrounding them with strict controls regarding privacy and accountability. It appears to the Committee that this aspect has been obscured where the issue of the B-party warrants is concerned.

4.55 The Committee considers that in addition to the requirements imposed under section 46(1)(a), (b), and (c) of the Act, the additional preconditions suggested by Professor Williams and Mr Blunn be included. The Committee is of the view that this will address the reservations expressed by the Law Council and EFA.

Recommendation 19

4.56 The Committee recommends that the Bill be amended to require that an applicant for a B-party warrant demonstrate:

- **evidence to support their belief that the information likely to be obtained from the intercept is material to the investigation; and,**
- **establish that it cannot be obtained other than by telecommunications interception or the use of a listening device.**

Recommendation 20

4.57 The Committee also recommends that the proposed section 46(3) (which contains the requirement that the issuing authority must not issue a B-party warrant unless he or she is satisfied that the agency has exhausted all other practicable methods of identifying the telecommunications services used) be amended to exclude the word 'practicable', to ensure that before a person is

38 *Committee Hansard*, 15 March 2006, p. 47.

subject to a B-party warrant no other way of approaching the problem is available.

Rolling warrants

4.58 The Committee heard from the Law Council that the 1979 Act included provisions for rolling over, or extending, interception warrants. The Law Council was concerned at the possibility that the same might apply to the B-party intercepts:

> When you think about rolling over interception warrants in relation to innocent people, the mind boggles. We believe that there should not be any rollover unless a judicial officer can be shown that some very useful or crucial information from an earlier warrant was gained.[39]

4.59 Rolling warrants allow a warrant to be renewed before the original warrant has expired. Their use is circumscribed, and the Attorney General's Department explained in evidence that provisions which apply to the stored communications warrants under this bill do not permit the use of rolling warrants for stored communications.[40] However, there does not appear to be a similar prohibition on rolling B-Party warrants.

4.60 The Committee considers, given the nature of these warrants, that the Bill should be amended to state specifically that the B-party interception warrants cannot be renewed under any circumstances. Instead, if further interception is required after a warrant expires, it should be the subject of a fresh application.

Recommendation 21

4.61 The Committee recommends that the Bill be amended to state that B-party interception warrants cannot be renewed. If further interception is required after a warrant expires, it must be the subject of a fresh application.

Dissemination and subsequent use: legal and other professional privilege

Use and derivative use

4.62 A principal problem with the B-party warrant is the potential for collecting a great deal of information which may be incidental to, or not even associated with the investigation for which the warrant was issued. As Senator Ludwig noted, 'it is not only the B-party but also the C, D E and F parties who may at some point end up talking to B and, therefore, being captured'.[41] The result is that potentially not just one, but a great many non-suspects to be caught in the B-party warrant process.

---

39 *Committee Hansard*, 15 March 2006, p. 29

40 *Committee Hansard*, 15 March 2006, p.40

41 *Committee Hansard*, 15 March 2006, p. 29.

4.63 The subsequent use of such material obtained does not appear to be controlled. This was confirmed to the Committee in response to a question from Senator Ludwig in which Mr McDonald of the Attorney General's Department affirmed that use and derivative use would be permitted of the material obtained under a B-party warrant relating to a non-suspect.[42]

4.64 Mr Gifford explained that this is consistent with the way that a service or named person warrant currently operates:

> … you may be the target of the interception and conversing with Senator Payne, and Senator Payne is not a target of the investigation at all. But Senator Payne may talk about another offence that was not the subject of the original investigation, to the extent that the original warrant was justified to and authorised by the issuing authority. Then any criminal intelligence which is subject to a three-year penalty threshold can be used.[43]

4.65 Mr Gifford explained the implications of limiting the use of this material. He continued:

> The reverse situation would require destruction of very valuable criminal information. The extreme example would be that you would happen upon some very valuable information in terms of a terrorism investigation. That is an extreme example, but the use of that information is useful for our operational agencies and has been justified in terms of the initial warrant being authorised by the issuing authority.[44]

4.66 It could be argued that the terms of the warrant itself would dictate the limits of the use of information obtained, but given the potential breadth of the information able to be sought under items 8 and 9 of Schedule 2 (amending section 46), and in the light of the remarks made by Professor Williams discussed above, it is likely that a great deal of what the Hon Duncan Kerr MP calls 'collateral information' will be collected, and therefore available for use.[45]

4.67 The Law Council of Australia, while maintaining its concerns regarding the B-party warrants, said that proper controls are necessary to regulate use and derivative use.[46] Professor Williams also supported stricter controls:

> My view is that it is better to be safe than sorry in an area like this, and it is very difficult through destruction only to be absolutely clear that the immunities you would expect to apply in such circumstances actually do apply. In the same way, it is common to see immunities, whether it be in the ASIO legislation or other bits of legislation, recognising that information

---

42 *Committee Hansard*, 15 March 2006, p. 51.

43 *Committee Hansard*, 15 March 2006, p. 51.

44 Ibid.

45 *Submission 1*, p. 4

46 *Committee Hansard*, 15 March 2006, p. 6.

> can be collected inadvertently, otherwise it should not have been collected. I would prefer to see a clear, direct statement indicating that, if it does not fit within the information that could have been collected for a certain purpose, immunities apply. I think it is inappropriate for enforcement agencies, simply through their luck or overboard legislation, to get access to information and then use it. [47]

4.68 Further, the fact that these warrants collect material about third parties who are not suspects must demand particular conditions about the use of any information obtained.

Professional privilege – legal and otherwise

4.69 A particular problem in this potentially open-ended process, concerns that of professional privilege. While the discussion centred upon legal professional privilege, the confidential nature of telephone contact with doctors, family members and other professionals was raised. Ms Irene Grahame[48] indicated that EFA already believes that there is a problem with the existing interception warrants and that the B-party warrants represent an even greater problem because of the issue of legal professional privilege. Ms Grahame continued:

> It is ridiculous to think that people would no longer be able to be confident in seeking legal advice because their lawyer's phone was being intercepted. … Any extension of it, in our view, would have to make very clear that B-parties could not cover lawyers, because there is too much potential for people who are not a suspect and the lawyer who is not the suspect having their calls intercepted. [49]

4.70 Ms Grahame also considered the possibility of such an exception also applying to other people who have a large number of calls, including politicians and accountants.[50]

4.71 Professor Williams took the view that:

> … unless there are particular or special circumstances, privileged information, such as lawyer-client information, ought not be collected through this type of regime. There are good arguments whereby, if lawyers themselves were involved in activity that may be criminal or otherwise, that may well negate the privilege. I could accept that there may be reasons why it should be collected on that basis. Otherwise, the very nature of lawyer-client privilege is that, where the government itself tends to be the party on the other side of the litigation table, it is highly inappropriate that the government gets access to that very information. It casts into doubt the

47 *Committee Hansard*, 15 March 2006, p. 30.

48 *Committee Hansard*, 15 March 2006, p.14

49 *Committee Hansard*, 15 March 2006, pp 9-10.

50 *Committee Hansard*, 15 March 2006, p.10

> justice system in terms of how that information is used. It can lower public confidence and, except in those limited circumstances, I would prefer to see a clear exception for that type of information.[51]

4.72 In pursuing this issue with the Attorney-General's Department, the Chair of the Committee asked about the interception of conversations between individuals and legal representatives, medical practitioners or clergy.[52]

4.73 In response, Mr McDonald of the Attorney General's Department indicated that in the case of *Carmody v MacKellar Ors*[53] the full Federal Court held that legal professional privilege was excluded by implication under the current warrant provisions of the TI Act. By extension, the privilege is excluded under the B-party warrant regime, even though these warrants are specifically directed against innocent parties.

Committee view

4.74 The Committee remains most concerned at the potential breadth of information relating to individuals suspected of no criminal offence which could be captured under the B-party warrants. The Committee does not consider that the provisions which operate for other warrants under the Act are adequate for this unique situation.

4.75 The Committee notes the comments made by Professor Williams in discussion of the use implications and those for legal professional privilege:

> I would prefer to see a clear, direct statement indicating that, if it does not fit within the information that could have been collected for a certain purpose, immunities apply. I think it is inappropriate for enforcement agencies, simply through their luck or overboard legislation, to get access to information and then use it.[54]

4.76 The Council for Civil Liberties agreed:

> [I]f you are going to provide this power then you need to provide an immunity so that anything that is not directly related to the investigation for which the warrant has been obtained needs to be expressly excluded from being used in evidence against anybody else.[55]

4.77 The Law Council's recommendations supported the need for limitations:

> g. The measures should contain express exemption categories. Exempt communications should include the confidential communications with lawyers, doctors and the clergy;

---

51 *Committee Hansard*, 15 March 2006, p. 29

52 *Committee Hansard*, 15 March 2006, p. 45.

53 [1997] 839 FCA

54 *Committee Hansard*, 15 March 2006, p. 30.

55 *Committee Hansard*, 15 March 2006, p. 58.

h. The proposed measures should expressly provide that Schedule 2 does not abrogate Legal Professional Privilege;[56]

4.78 The Committee is aware that these amendments are designed to meet some of the demands which are a function of modern technology, and acknowledges that law enforcement agencies are constantly meeting situations which demand sophisticated technical responses. Nevertheless, it is important to keep in mind the purpose behind the principle of legal professional privilege: that the law and the system of justice that administers it, is complex and that those affected by it are in need of professional assistance. In seeking such assistance, the client must be able to reveal all the relevant facts without inhibition, in order to get effective advice.[57]

4.79 So long as the communications are legitimately for the purpose of gaining professional legal advice, they should be protected in the normal way. In addition, there is little benefit in creating rules against the admissibility of such evidence if, in fact, law enforcement agencies have been privy to the confidential information already.

Recommendation 22

4.80 The Committee recommends that Schedule 2 be amended to provide that certain material obtained under a B-party warrant will be exempted from use under the legislation. This material should include bona fide communications between solicitor and client; clergy and devotee; doctor and patient and communications by the innocent person with any person other than the person of interest to the law enforcement agency.

Recommendation 23

4.81 The Committee further recommends that the Bill be amended to introduce defined limits on the use and derivative use of material collected by B-party warrant.

Reporting and accountability requirements

4.82 A matter of vital importance to the workability of the proposals is the strength of the reporting and accountability regime, particularly in view of the covert nature of the warrant system proposed. Warrants granted under Part III and Part VI would have differing reporting and accountability requirements.

B-party warrants issued on application of the Director-General of Security

4.83 The Inspector-General of Intelligence and Security has a statutory obligation under the *Inspector-General of Intelligence and Security Act 1986:*

56 Submission 17, pp 3-4.

57 Gillies, P., *Law of Evidence in Australia*, p. 433.

a) to assist Ministers in the oversight and review of:

(i) the compliance with the law by, and the propriety of particular activities of, Australian intelligence or security agencies;

(ii) the effectiveness and appropriateness of the procedures of those agencies relating to the legality or propriety of their activities; and

(iii) certain other aspects of the activities and procedures of certain of those agencies;

(b) to assist Ministers in ensuring that the activities of those agencies are consistent with human rights; and

(c) to allow for review of certain directions given to ASIO by the Attorney-General. [58]

4.84 There is no existing requirement for telephone intercept warrants issued by the Attorney and associated documents to be destroyed, but monitoring and inspection regimes do apply.

4.85 In his submission to this inquiry, Mr Ian Carnell, the Inspector-General of Intelligence and Security indicated that his office conducts monthly inspections of all requests by ASIO for telecommunication interception (including named person) warrants under the TI Act.

> In addition to this, the office of the IGIS also inspects all requests for questioning and detention, entry and search, listening device, computer access and computer access warrants sought under the *Australia Security Intelligence Organisation Act 1979* (ASIO Act).[59]

4.86 In scrutinising ASIO's requests for warrants, the office of the IGIS checks *inter alia*, that the intelligence or security case is soundly based, and all appropriate internal and external approvals have been obtained.

4.87 The scrutiny also extends to the timely provision of factual reports to the Attorney-General of the outcome of executed warrants and checking that the activity concerned occurred only during the approved period.

4.88 Mr Carnell noted that both the B-Party interception and equipment-based interception will be subjected to this inspection regime; he also observes that:

> … the nature of B-Party interception warrants inherently involves a potential for greater privacy intrusion for persons who may not be involved in activities of legitimate concern under the ASIO Act. As a result, particular attention will be given to the additional legislative tests for this type of warrant. As a result, particular attention will be given to the

58 Section 4

59 *Submission* 9, p. 2.

> additional legislative tests for this type of warrant, as well as checking that the duration of 90 days is adhered to.[60]

B-party warrants issued on the application of a law enforcement agency

4.89 For the B-party warrants issued by Judges and members of the AAT, the reporting, destruction and supervising arrangements are the same as those which currently apply to telephone intercepts. Briefly, sections 79, 80 and 81 prescribe the circumstances under which records are to be destroyed, and the records that must be kept of notifications and certification of warrants, outcomes and use of information obtained under the warrant.

4.90 In evidence, Mr Gifford of the Attorney General's Department explained:

> The use and destruction provisions that are currently in the existing *Telecommunications (Interception) Act* will apply to B-party interception. It was a conscious decision by the Attorney-General that they would be maintained… The *Telecommunications (Interception) Act* currently requires the destruction of material once the general and special registers of warrants have been inspected by the Attorney-General. Those registers are compiled three-monthly by the AFP. After they are reviewed and signed off by the Attorney-General then a notice is provided to all agencies, at which point they may destroy all material that is contained in the general and special registers.[61]

4.91 The Explanatory Memorandum to the Bill explained:

> Lawfully obtained information obtained as a result of B-Party interception will be subject to the existing destruction provisions of the Act, namely, destruction where the permitted purpose for use cease to exist.[62]

Criticisms of the accountability regime

4.92 Several submissions pointed to weaknesses in this regime. Electronic Frontiers Australia said in their submission that the current arrangements for destruction have been ineffective since 2000:

> The existing destruction provisions apply only to 'restricted records' which has not included copies of intercepted communications since amendments made in 2000. Hence copies of irrelevant intercepted information, e.g. communications between the innocent B-Party and other innocent persons, will be permitted to be retained forever due to the inadequate destruction provisions of the existing Act.[63]

---

60 Submission 9, pp 2-3.

61 *Committee Hansard*, 15 March 2006, pp 50-51.

62 Explanatory Memorandum to the Telecommunications (Interception) Amendment Bill 2006, p. 32.

63 *Submission* 3, p. 28.

4.93 The Privacy Commissioner also expressed disquiet at the provisions for destruction, recommending 'enforceable, audited requirements that any intercepted material outside the scope of the purpose stated in the warrant be immediately destroyed.'[64]

4.94 The Law Council[65] and EFA[66] made substantively similar recommendations which suggested that the government should be required to report annually on specific details of B-party warrants including:

- the number and justification of B-party intercept warrants (which should be separately recorded by the Agency Co-ordinator and reported to the Attorney General);
- the number of warrants issued by the Attorney General, judicial officers and nominated AAT Member pursuant to schedule 2, and including the grounds upon which they were issued;

4.95 EFA also recommends that the reporting requirements should include the suggestion made in the Blunn report that destruction of non-material content in whatever form should be strictly supervised. [67]

4.96 The Committee endorses the proposals to improve security and accountability in relation to B-party warrants, and reiterates its view that the proposals cannot be treated as being analogous to the current TI warrant arrangements.

Recommendation 24

4.97 The Committee recommends that:

- **there should be strict supervision arrangements introduced to ensure the destruction of non-material content in any form;**
- **the number and justification of B-party intercept warrants should be separately recorded by the Agency Co-ordinator and reported to the Attorney General; and**
- **the use of such warrants should be separately reported to the Parliament.**

Role of the Ombudsman

4.98 A further consideration that relates specifically to law enforcement agencies is the role of the Commonwealth Ombudsman. The overall inspection of interception warrant records is the responsibility of the Ombudsman under Section 82 of the *Telecommunications (Interception) Act 1979*. Under the Act, the Ombudsman's role is

64 *Submission* 6, p. 2.

65 Submission 17, p. 4

66 *Committee Hansard*, 15 March 2006, p. 9

67 *Submission* 3, p. 28

to inspect and report on the records of telecommunications interception activity by the Australian Federal Police and the Australian Crime Commission.[68]

4.99 The Ombudsman explained:

> Section 83 of the Act requires the Ombudsman to inspect each of these agency's records at least twice in each financial year to ascertain the extent to which they have complied with the provisions of sections 79, 80 and 81 of the Act dealing with the destruction and maintenance of records. Under section 85, the Ombudsman may also report on any other breaches of the Act detected in the course of an inspection. Under section 84, the Ombudsman is required to report to the Minister within three months after the end of each financial year about the results of the inspections conducted under section 83 in relation to each agency during that financial year. As a consequence of amendments to the Act which came into effect in July 2005, I am now required to include in my annual report to the Minister particulars of any deficiencies identified in those inspections that may impact on the integrity of the telecommunications interception regime and particulars of any remedial action taken or proposed to address those deficiencies.[69]

4.100 While there are no specific requirements for the Ombudsman to investigate particular aspects of the B-party warrants subject to certain provisions of the Act, the Ombudsman can undertake own motion investigations under the *Ombudsman Act 1976* into other matters relating to the conduct of telecommunications interceptions by law enforcement agencies.

4.101 It is theoretically open to any person adversely affected by the B-party warrant provisions to notify the Ombudsman, in the case of an agency, or the IGIS in the case of an ASIO warrant. However, the nature of the provisions and the covert nature of the surveillance makes it most unlikely if not impossible for such a notification to occur. As the Committee Chair noted in the public hearing:

> I am not entirely persuaded that one can complain to the Ombudsman or the IGIS about a telephone intercept that one does not know about. [70]

4.102 As discussed in the previous chapter, in view of the additional warrants which the Ombudsman is required to inspect and report on, the Committee is concerned to ensure that sufficient resources are at the Ombudsman's disposal. The Ombudsman remarked:

> The Ombudsman's inspection and reporting role is an important safeguard in ensuring that these powers are not misused and in maintaining public confidence in the integrity of the new warrant regime. It would be contrary

68 *Submission* 10, p. 1.

69 Ibid.

70 *Committee Hansard*, 15 March 2006, p. 50.

> to the intent of the legislation if this office were forced to curtail these activities for want of resources to fulfil this role.[71]

4.103 The Ombudsman continued:

> Whether my office is able to inspect most, if not all, agencies, in the spirit of the proposed amendments, or whether we will be able to inspect only a few, will depend on whether additional resources are available. Not only will staff need to be available to carry out inspections but preparatory work on methodologies and the internal procedures of each agency to be inspected will need to be done. If the resources are available to meet both my mandatory inspection obligations and my function under proposed section 152, my aim would be to have a program of inspections covering all agencies which have accessed stored communications in the relevant year. [72]

4.104 Accordingly, the Committee reiterates its previous recommendation relating to the adequacy of funding to the Commonwealth Ombudsman.

Review of the legislation

4.105 A number of submittors and witnesses suggested that there should be a review of the legislation after a period of time, or the inclusion of a sunset clause.

4.106 The Law Council of Australia said that 'similar to other legislation which erodes fundamental rights of the Australian people', Schedule 2 should be subject to independent review, for instance, two or three years after its commencement; and 'a sunset clause should be incorporated in the Act'.[73]

4.107 In evidence, Mr Cameron Murphy of the Council for Civil Liberties agreed that a sunset clause coupled with a review would ensure that the conditions which support the introduction of these provisions are continuing.[74]

4.108 Mr Blunn's report considered further reviews inevitable:

> Indeed given the rate of changes within the industry and within society more generally I believe that there is a strong case for regular reviews, say at three yearly intervals. The complexity and significance of the issues makes it problematic for unversed persons to do justice to them within a reasonable time frame. I am not a fan of committees but there may be

71 *Submission* 10, p. 4.

72 Submission 10, p. 2

73 *Submission* 17, p. 3.

74 *Committee Hansard*, 15 March 2006, pp 59-60

> advantage in there being a standing representative committee structure which could do or at least provide support for future reviews.[75]

4.109 Dr Clapin, from the Office of the Privacy Commissioner said in evidence that such a review should not be limited to these provisions, but to the entire Act and that provision should be made in these amendments.[76]

Committee view

4.110 The Committee considers a sunset clause to be appropriate for the B-party interception warrant provisions; it would serve as a catalyst for a review of the whole telecommunications interception structure, and in the light of advancing technology would offer an opportunity to assess the adequacy or otherwise of this regime.

Recommendation 25

4.111 The Committee recommends that the Bill should include a provision for the provisions to expire in five years, with a review at that time or earlier.

4.112 The Review should encompass the broader issues surrounding the suitability and effectiveness of AAT members in the warrant issuing regime, together with consideration of ways in which the Act may be amended to take account of emerging technologies such as peer-to-peer technology.

Equipment based interception

4.113 Schedule 3 to the bill deals with the provisions concerning equipment-based interception.

4.114 Under current law, it is possible to apply for a TI warrant for a named person, which allows interception of phone services attached only to that particular person rather than to a specific device. This has been a source of difficulty for law enforcement agencies, when targets of interception use a multitude of different SIM cards or phone numbers that may not be registered in their name.

4.115 The Explanatory Memorandum states:

> The purpose of this Schedule is to amend the named person telecommunications interception warrant provisions to enable interception agencies to intercept communications to and from communications equipment such as mobile handsets and computer terminals. These amendments are designed to assist interception agencies to counter measures undertaken by persons of interest to evade telecommunications interception such as adopting multiple telecommunications services.[77]

---

75 Blunn, p. 2.

76 *Committee Hansard*, 15 March 2006 p. 22.

77 Explanatory Memorandum, p. 34.

4.116 The proposed warrants will only be issued where the agency can show that there are no other practicable methods of identifying the device. The issuing authority must be satisfied that the applicant agency 'has no practicable methods of identifying the telecommunications services used or likely to be used by the person of interest, or that interception of those services would not be possible.'[78]

4.117 The provisions are designed to gain access to an individual piece of equipment-such as a computer or a mobile phone, via a unique identification number. In evidence, Ms Hume from the Attorney General's Department explained:

> Proposed section 6Q in schedule 3 … talks about the identification of a telecommunications service. In both subsections (a) and (b) it refers to a unique telecommunications number. In item 3 the list of those numbers shows that potentially it could be a telephone number. It could be an IMEI[79] … It could be a MAC address of a computer. But that provision, 6Q, specifies that it has to be unique; it is a unique telecommunications number.[80]

4.118 However Electronic Frontiers Australia considered that such unique identifiers are unreliable. The submission recommended that the Schedule be deleted from the bill:

> This proposal appears to have an inappropriately and unjustifiably high potential to result in interception of communications of persons who are not suspects (i.e. are not named in the warrant) because, among other things, the types of device numbers proposed to be used do not necessarily uniquely identify a particular device.[81]

4.119 EFA notes that while the Blunn report briefly discussed equipment-based interception proposals, he made no recommendation that the warrants be implemented. Rather, his recommendation proposed:

> that priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.[82]

4.120 In evidence, it became clear that there was a sound basis for EFA's concerns. Mr Gifford of the Attorney General's Department acknowledged that there is potential for duplication of numbers thought to be unique:

> We do understand that risk, and we are aware that there are duplicate IMEIs in a telecommunications network. On that basis, we have said, 'When you're seeking interception on the basis of a handset, it must be defined by reference to a unique telecommunications number, which, for the purposes

78 Ibid.

79 International Mobile Equipment Identifier

80 *Committee Hansard,* 15 March 2006, p. 55

81 EFA, *Submission 3*, p. 28

82 Blunn, p. 46.

> of the definition, will include an IMEI. … You must satisfy the issuing authority that the IMEI you are seeking interception of is a unique IMEI number.[83]

4.121 Deputy Commissioner Lawler explained that:

> … we have seen a practice whereby these numbers have been copied fraudulently within service providers to commit fraud, but also to enable another way of not being able to identify who has the particular handset in question. I understand from the briefings I have received that there is the capacity to remove such duplicate numbers from the system, as there is also the capacity to remove stolen handsets from the system. As has been indicated, we would do the checks that are required for the potential for those numbers to be duplicated on the system, but they are only duplicated through, as I am briefed, a fraudulent activity and the numbers being cloned or copied.[84]

4.122 In further discussion, the AFP indicated that they would be required to undertake inquiries regarding the uniqueness of the proposed identifier, and to provide details in any application for a warrant the steps which had been undertaken to achieve this.[85] The Committee notes that it was not clear from the evidence the extent to which that process would guarantee that the device being targeted under the warrant was able to be certified as uniquely identifiable.

4.123 The Privacy Commissioner also had reservations about Schedule 3, observing that it 'broadens the ways in which law enforcement agencies may seek to intercept communications under the Interception Act.'[86] While acknowledging that the proposals offer a practical solution in instances where multiple SIM cards are used on the one handset:

> … the provisions in Schedule 3 appear to move beyond just permitting interception of particular mobile phone handsets, for example in permitting telecommunications equipment to be identified on the basis of an email address or a 'user account identifier'.[87]

4.124 The Privacy Commissioner concluded:

> The Office has not been able to fully determine the limits to the scope of the operation of Schedule 3, and so recommends that careful consideration be given to ensuring that the provisions of Schedule 3 do not give rise to an unintended reduction of the privacy protections in the Interception Act.[88]

---

83 Mr Gifford, *Committee Hansard*, 15 March 2006, p. 54

84 Federal Agent Lawler, *Committee Hansard*, 15 March 2006, p. 54

85 *Committee Hansard*, 15 March 2006, p. 55

86 *Submission* 6, p. 3.

87 Ibid

88 Ibid

Committee view

4.125 The Committee considers that any arrangement designed to target a specific piece of equipment should be able to identify it with a high degree of certainty. It is the Committee's view that while there is a clear operational requirement for law enforcement agencies to be able to target specified devices, doubts remain over their capacity to identify these devices with a high degree of certainty. As Mr Blunn recommended, priority should be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access. However, the Committee also recognises that such developments may take some years to achieve and does not consider it practicable to delay the passage of the provisions until that time.

Recommendation 26

4.126 The Committee recommends that the recommendation contained at paragraph 3.2.5 of the Blunn report be adopted, and priority given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.

CHAPTER 5

OTHER AMENDMENTS

5.1 This chapter considers the remaining provisions of the Bill:

- The removal of the distinction between Class 1 and Class 2 offences.
- The removal of the TIRAC function.
- Items in Schedule 6.

Class 1 and 2 offences

5.2 Until now the interception regime has authorised interception on the basis of classes of offences. In the past only Class 2 offences required the issuing authority to have regard to privacy considerations. The offence distinctions have been removed and the offences are now termed 'serious offences'. Serious offences are defined in the new section 5D, and include murder or similar offences, kidnapping, offences under Division 307 of the Criminal Code (these include importation and possession of certain drugs and plants) terrorism offences, offences against Division 72, 101, 102 or 103 of the Criminal Code (terrorism offences); or an offence in relation to which the ACC is conducting a special investigation.

5.3 In his report, Mr Blunn explored the necessity for the classification of offences for the purposes of obtaining TI warrants. He found that law enforcement agencies found the classification 'over prescriptive' and occasionally a barrier to accessing data rather than a support.

5.4 The report continues:

> Given that the objective in the case of both Class 1 and Class 2 offences is to justify the issuing of an interception warrant and having regard to the similarity of the offences it is not clear why the distinction is made. Any significance can only be in terms of the processes relating to the issue of a warrant. The only difference between those processes is that in relation to Class 2 offences the issuing authority is required to have regard to the gravity of the offence and the extent of the interference to privacy involved. In the case of Class 1 the gravity of the offences is inherent and presumably is regarded as over-riding any privacy considerations.[1]

5.5 He concluded that the provision produces no meaningful difference in outcome, and adds to the length and complexity of an already convoluted Act. He recommended that 'those offences currently described as Class 1 and Class 2 offences be identified solely by reference to the prescribed term of imprisonment'.[2]

---

1 Blunn, p. 55.

2 Ibid.

5.6 The removal of the distinction was commented upon by the Law Council. The Council had serious reservations about much of the Bill, and considered that particularly in the case of B-Party intercepts, the existing Class 1 offences should be the only offences which allowed the issue of a warrant.[3]

5.7 Conversely, both the AFP[4] and Commissioner Hyde of the South Australian Police supported the proposal. Commissioner Hyde further suggested that:

> Another class of offence to capture corruption, child pornography and significant offending that does not carry a 7 year term of imprisonment should also be considered.[5]

5.8 The Explanatory Memorandum notes that the amendments are designed to 'simplify a complex area of the interception regime'. The Committee notes the Commissioner's suggestion, but considers that to add another class of offences at this point would defeat the purpose of simplification. Nevertheless, the offences he refers to are of sufficient seriousness that they may warrant consideration in any subsequent review of these provisions.

5.9 In general, the effect of the amendments is to bring privacy considerations to all warrant applications and not limit them to class 2 offences. The Committee welcomes this enhancement of the privacy protections available under the Act.

Removal of the TIRAC function

5.10 Schedule 5 of the Bill repeals the Telecommunications Interception Remote Authority Connection (TIRAC) function which is exercised by the AFP. The removal of this function from the AFP was a recommendation of the Blunn report.

5.11 TIRAC is described in the Explanatory Memorandum as

> … a historical electronic accountability mechanism which requires each interception agency to lodge its interception warrants with the AFP. The effect of this function is that the warrants do not take effect until the AFP receives the warrant and notifies the Managing Director of the carrier of the issue of the warrant.[6]

5.12 In his second reading speech, the Attorney General observed that:

> TIRAC's utility has been exhausted by technological developments, and the bill replaces the current requirements for AFP to facilitate warrants by a requirement for my department to scrutinise warrants immediately upon issue and maintain a register of warrants.

---

3 *Committee Hansard*, 15 March 2006, pp 2-3.

4 *Committee Hansard*, 15 March 2006, p. 32.

5 *Submission 16*, p. 3.

6 Blunn, p. .

> The act will continue to require all agencies to maintain comprehensive records as part of the interception regime which are subject to regular compliance inspections by the Commonwealth Ombudsman or equivalent state oversight body.[7]

5.13 This amendment, which is effectively an administrative one, was supported by the AFP, and was not a subject which elicited a great deal of comment by submitters or witnesses. The Committee considers that the change should be monitored to ensure that the effect of the amendments does not lower standards of efficiency or accountability.

Other amendments: Schedule 6

5.14 Schedule 6 of the Bill makes other amendments to the Act to ensure the ongoing effective operation of the interception regime in Australia.

5.15 The proposed amendments seek to:

- include an additional permitted purpose for use and communication of lawfully obtained information in relation to the Victorian Office of Police Integrity;
- clarify that employees of a carrier exercise authority under a telecommunications interception warrant when assisting law enforcement agencies in the execution of interception;
- remove the exception to the definition of interception in subsection 6(2) of the Act;
- update applicable reference to money laundering offences in New South Wales; and
- correct drafting errors within the Act which have been the result of previous amendments Acts.[8]

5.16 Generally, the amendments contained in Schedule 6 of the Bill have not been the subject of any objection throughout the inquiry.

5.17 One minor exception is the repeal of subsection 6(2).

5.18 Subsection 6(2) creates an exception to the general prohibition in subsection 7(1) against the interception of a communication in its passage of the Australian telecommunication system. At the commencement of the Act subsection 6(2) was intended to exempt the activities of telecommunications carriers and employees of the carrier from the general prohibition contained in subsection 7(1) to allow the testing of

---

7 *House of Representatives Hansard*, 16 February 2006, pp 9-10.

8 Explanatory Memorandum, p. 47.

the carrier's equipment to ensure that the network and associated equipment operated correctly.[9]

5.19 The Australian Bankers Association states that:

> Section 6(2) is consequently most useful in the context of emails where it is not possible to ensure that the person making the communications has 'knowledge' of any recording or listening activities. The repeal of the section may therefore impact on the ability of organisations to monitor incoming emails. This is a matter of grave concern in light of the need for organisations to perform, for various reasons, the routine interception and scanning of such communications.

5.20 However, the repeal of subsection 6(2) has been welcomed by many organisations. The Office of the Privacy Commissioner advised that:

> The Office supports the repeal of s. 6(2) of the Interception Act. This section has given rise to confusion in the past about the circumstances under which phone calls may be covertly monitored. The repeal of s. 6(2) will assist in reinforcing the privacy objects of the Interception Act.

5.21 Proposed section 108(2) sets out a number of exceptions to the general prohibition on access to stored communications. Subsection 108(2)(e) provides that the general prohibition does not apply in relation to:

> Accessing a stored communication by another person lawfully engaged in duties relating to the installation, connection or maintenance of equipment or a line, if it is reasonably necessary for the person to access the communication in order to perform those duties effectively

5.22 The Explanatory Memorandum states that:

> This exception provides that network or system administrators do not contravene the prohibition against interception by performing routine functions designed to prevent malicious content such as viruses from entering their networks.

Committee view

5.23 The Committee considers that the concern expressed that the repeal of subsection 6(2) impacts the ability to monitor incoming emails is addressed by the proposed exemptions to the general prohibition on stored communications in subsection 108(2).

5.24 The Committee also agrees with the view that the repeal of the subsection reinforces the privacy objectives of the Act.

---

9 Explanatory Memorandum, p. 48.

Recommendation 27

5.25 The Committee recommends that the amendments proposed in Schedule 6 of the Bill be passed.

Recommendation 28

5.26 Subject to the amendments set out above, the Committee recommends that the Bill be passed.

Senator Marise Payne
Committee Chair

SUPPLEMENTARY REPORT WITH ADDITIONAL COMMENTS OF DISSENT BY THE AUSTRALIAN DEMOCRATS

1.1 The Democrats agree with a majority of the recommendations presented in the Chair's report.

1.2 We commend the Chair and the Secretariat for their efforts.

1.3 The Democrats recognise the importance of the review of the regulation of access to communications carried out by Mr Anthony Blunn AO and agree that it is necessary that amendments be made to the current outdated *Telecommunications (Interception) Act 1979* in order to maintain its technological relevance.

1.4 We note with dismay the lack of time that the committee has been allocated to report on this bill. The ability of members of the general public to make submissions and Senators to report to the Parliament is constrained when there is inadequate amount of time to consider a Bill.

1.5 We believe the Bill, as introduced, does not adequately account for privacy considerations.

1.6 The operation of the Bill is in conjunction with other legislation which further reduces fundamental civil liberties of Australian citizens.

1.7 We believe a majority of the recommendations contained in the Chair's report will improve the Bill and lessen the potential for abuses of privacy but provide the following additions:

Stored Communications Warrants – Schedule 1

1.8 The Democrats recognise the necessity for a stored communications warrant regime to be introduced in order to maintain the ability of enforcement agencies to efficiently combat crime.

1.9 We believe that the balance between the privacy rights of Australians and the need for enforcement agencies to carry out their duties efficiently is disproportionate in the current format of the bill to the detriment of privacy rights.

1.10 A matter of concern for the Democrats is the differing thresholds for interception warrants and stored communications warrants.

1.11 During the inquiry, I asked the Attorney-General's Department about the rationale for the differing thresholds for stored communications and interception warrants. The notion that e-mails and SMS' are more considered than a live communication was stated by the Department;

> "It is something that is in writing – something that definitely involves more consideration of the expression – although there is the speed issue."[1]

This rationale is unconvincing. In response to this claim, Professor Williams argued;

> "It strikes me as nonsensical that a differentiation would be drawn between speaking to somebody on a mobile phone and sending them an SMS message. Many of the students who I teach today see them as equivalent forms of communications. It makes no sense as a matter of law or public policy why, indeed, it is easier to gain one type of information than the other … I think the proper focus for assessing this legislation is: what is the appropriate limitation upon the privacy of Australian people? For them there is no rational distinction, so I cannot see how you could justify one from the government's end."[2]

1.12 I note statements made earlier in the year by NSW Council of Civil Liberties Chair Mr Cameron Murphy regarding comparisons of Telecommunication Intercepts between Australia and the United States where he highlighted the councils concerns:

> "Recently released figures show that telephone wiretapping by government agencies in Australia (including the police) continues to grow. Not only does Australia issue 75% more telecommunications interception warrants than the US, but per capita Australia issues 26 times more warrants than the US. In Australia non-judges issue 76% of all warrants, whereas in the US only judges can issue warrants.
>
> In the twelve months 2003/2004 there were 3028 warrants issued in Australia. In the twelve months of 2004, US courts issued 1710 warrants. Adjusting for population, Australia intercepts telephone communications 26 times more per capita than the United States.
>
> Worryingly, the numbers are way up on figures only two years ago. In 2001 there were more than 2150 warrants issued in Australia, compared with only 1490 warrants issued in the United States of America. Australia intercepted telephone communications 20 times more per capita than the United States."[3]

1.13 The Democrats see these overwhelming numbers as an indication that the current methods of oversight are not functioning properly.

1.14 The Democrats support the recommendation made by the Chair to review the suitability and effectiveness of the AAT in warrant issuing regime.

1.15 In order to address these deficiencies we make the following recommendations;

Recommendation 1

1.16 That the threshold for stored communications warrants, that being for investigations into offences with penalties of at least a maximum of three years,

---

[1] *Committee Hansard*, Wednesday, 15 March 2006, p. 39.

[2] *Committee Hansard*, Wednesday, 15 March 2006, pp. 28 and 31.

[3] NSW Council for Civil Liberties, 'Australia phones 26-times more likely to be bugged than an American phone', *media release*, 13 January 2006.

be replaced by the same threshold as that for telecommunication interception warrants.

Recommendation 2

1.17 That more information be required of agencies requesting a stored communication warrant. This information should include the number of previous applications the agency has made with respect to the person or the service the person has used, the number of warrants previously issued and the date on which the most recent was issued and particulars of the use made by the agency of information obtained by access under such warrants.

Recommendation 3

1.18 That the individuals on whom a stored communications warrant has been exercised be notified of the existence of the warrant where that disclosure will not materially affect the investigation. Where it is considered that such disclosure will materially affect the investigation, there exists an obligation on the Chief Officer of the agency to inform the person on whom the warrant was exercised as soon as that disclosure is considered to no longer materially affect the investigation.

B-Party Warrants – Schedule 2

1.19 The operation of B-party warrants represents a serious breach of privacy as they are targeted at non-suspected persons. We believe that the operation of B-Party warrants as they are contained in the Bill can not be justified.

1.20 As the Victorian Privacy Commissioner stated;

> "Telecommunications is one of the common means by which many individuals discuss their most private and intimate thoughts, as well as the ordinary daily details of their lives. They may also engage in political discourse, discuss business ventures, seek legal and other professional advice. People have a legitimate and reasonable expectation that the State will not listen surreptitiously to these conversations. Accordingly, any such interception has been subject to strict regulation under law, with oversight."[4]

1.21 The Democrats welcome the recommendations made in the Chair's report, however, we believe that the recommendations are not sufficient to ensure the privacy rights of Australian citizens.

1.22 During the inquiry, I asked a number of the witnesses for their opinion on how this Bill may operate in conjunction with other legislation to affect the civil liberties of Australian Citizens. Dr Bibby of the New South Wales Council for Civil Liberties stated;

---

[4] Office of the Victorian Privacy Commissioner, *Submission to the Commonwealth Parliament's Senate Legal and Constitutional Committee on its inquiry into the Provision of the Telecommunication (Interception) Bill 2004*, 12 March 2004.

> "As soon as you give powers to organisations to take away liberty in the way that the two antiterrorism laws and the powers that were given to ASIO a few years ago have done, you open up the possibility of it being done for totally spurious reasons. The more you allow privacy to be invaded, and the more you allow the stuff to be kept secret, the greater the chances are that these powers will be misused – and misused in ways which it is impossible for people to correct."[5]

1.23 The President of the New South Wales Council for Civil Liberties Mr Cameron Murphy remarked that;

> "We are seeing both the public and the parliament becoming desensitised to the nature of the extraordinary powers that are being sought. Instead of just being used to get us over a period in which there might be a drastic and imminent threat, it is becoming the norm, and those powers are being extended to many other agencies."[6]

1.24 The Democrats note this statement with alarm.

1.25 We believe that the Bill does not adequately consider the importance of professional privilege and note that where this privilege is abrogated it erodes the ability of lawyers, medical officers, parliamentarians and religious leaders to offer their services in confidence.

1.26 Despite arguments submitted by the Attorney-General's Department that there has been precedent established in *Carmody v MacKellar& Orrs* [1996] 791 FCA 1, which allows for the abrogation of legal professional privilege, we are not convinced that this should be applied by analogy to justify the interception of telecommunications to non-suspected third persons.

1.27 We believe that professional privilege should be protected from interception not only for the reason that non-suspected persons should not have their privacy infringed upon but also for reasons of public policy. It is crucial that Australian citizens can be assured that whatever information is given in confidence to a lawyer, religious leader or medical officer remains in confidence.

1.28 Evidence has been produced to persuade the Parliament that B-Party warrants are necessary in the prevention of crime and terrorism as criminals are evolving with technology and continuing to use it to their advantage to avoid detection and prosecution.

1.29 ASIO's ability to use B-party warrants is of concern to the Democrats as the criteria to obtain a warrant for the organisation operates at a very low threshold. Professor George Williams in his submission to the inquiry stated;

> "B-party warrants may be issued even if there is no evidence that the warrant will assist in obtaining information relevant to the activities which triggered the warrant. It is enough to show that intercepting B-party communications to or from *anyone* may assist in obtaining *any* intelligence related to security.

---

[5] *Committee Hansard*, Wednesday, 15 March 2006, p. 57.

[6] *Committee Hansard*, Wednesday, 15 March 2006, p. 57.

> Once it is shown that the person involved in activities prejudicial to security communicates with the B-party, the Director General must only discharge the very low burden that the interception will be likely to assist in obtaining intelligence related to security. 'Likely to assist' is a very broad standard. Further, the concept of 'relating to security' is both wide and vague, particularly since 'security' has the same wide meaning as that given in section 4 of the *Australian Security Intelligence Organisation Act 1979* (Cth)."[7]

1.30 The Democrats are of the belief that it is in only very remote circumstances where the use of a B-Party warrant may assist intelligence and enforcement agencies in a manner which would be otherwise unavailable to them.

1.31 For this reason, it is crucial that a high threshold be required in the issuing of a B-Party warrant. Any warrant issued should meet the following list of recommendations at a minimum.

Recommendation 4

1.32 The same requirements that apply to the AFP for a B-party warrant should also apply to ASIO.

Recommendation 5

1.33 The use of such warrants should only be authorised by a Judge on the Federal Court of Australia, the Family Court of Australia or on the Federal Magistrates Court.

Recommendation 6

1.34 Warrants should be limited to fourteen days duration and should not be renewable unless during that fourteen days information material to the investigation had been obtained and suggested that continued interception would likely result in further material information. The duration of a renewed warrant should not exceed 30 days.

Recommendation 7

1.35 An issuing authority must under no circumstances grant a B-Party warrant where the warrant is likely to breach professional privilege. Any agency applying for a B-Party warrant must state in an affidavit that they are of the belief that the B-party is not privy to professional privilege.

Recommendation 8

1.36 The B-Party must be informed about the operation of the warrant after it has been exercised. The Chief Officer of the authorised agency may use their discretion to delay the disclosure where such disclosure may materially affect the success of the investigation. Where disclosure will not materially affect the success of the case the Chief Officer is required to inform the B-Party of the existence of the warrant as soon as possible.

---

[7] *Submission 2*, p. 2.

Recommendation 9

1.37 No copies of recordings should be made before the review of the original recording. Where it is apparent that the interception does not involve the suspected person the recording should be immediately destroyed.

Recommendation 10

1.38 The destruction provisions of the act should be amended to mirror those contained in the *Surveillance Devices Act 2005.*

Equipment Based Warrants – Schedule 3

1.39 The section of the Bill that relates to equipment based warrants has led to much confusion as to the scope of its operation.

1.40 During the inquiry, I asked the Office of the Privacy Commissioner about their submission which stated;

> "The office has not yet been able to fully determine the limits to the scope of the operation of schedule 3."[8]

In response Mr Timothy Pilgrim, Deputy Privacy Commissioner stated

> "…it is an issue that we have been grappling with and, given our time to be able to devote to issues such as this, have not been able to fully explore…What we are not able to grapple with – or have not had time to grapple with – is how that might be broadly applied in various scenarios."[9]

1.41 Electronic Frontiers Australia in its submission stated that;

> "This proposal appears to have an inappropriately and unjustifiably high potential to result in interception of communications of persons who are not suspects (i.e. are not named in the warrant) because, among other things, the types of device numbers proposed to be used do not necessarily uniquely identify a particular device.[10]

1.42 The Democrats note that the Blunn report did not recommend the introduction of equipment based warrants. Rather the report recommended that "priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access."[11] Discussion in the report highlights the difficulties of accurately identifying a person through the use of International Mobile Service Identifiers (IMSI) or similar identification numbers.

---

[8] *Submission 6,* p. 3.

[9] *Committee Hansard,* Wednesday, 15 March 2006, p. 25.

[10] *Submission 3,* p. 29.

[11] Anthony Blunn AO 'Report of the Review of the Regulation of Access to Communications' August 2005

1.43 The Democrats believe that the operation of schedule 3 of the Bill in its current form is untenable and needs to be referred for further consideration.

Recommendation 11

1.44 Schedule 3 of the bill should be removed from the Bill and referred back to the committee until such time as it is possible to determine the full scope of its operation.

Senator Stott Despoja
Australian Democrats

APPENDIX 1

SUBMISSIONS RECEIVED

1	The Hon Duncan Kerr SC MP
2	Gilbert + Tobin Centre of Public Law
3	Electronic Frontiers Australia Inc.
3A	Electronic Frontiers Australia Inc.
4	Australian Privacy Foundation
5	New South Wales Council for Civil Liberties Inc
6	Office of the Privacy Commissioner
6A	Office of the Privacy Commissioner
7	Privacy NSW
8	Australian Competition and Consumer Commission (ACCC)
9	Inspector-General of Intelligence and Security
10	Commonwealth Ombudsman
11	WAPOL
12	Commonwealth Director of Public Prosecutions
13	Australian Securities and Investments Commission
13A	Australian Securities and Investments Commission
13B	Australian Securities and Investments Commission
14	Australian Bankers Association
15	The Law Society of South Australia
16	South Australia Police
17	Law Council of Australia
18	Australian Communications and Media Authority

19 Australian Customs Service

20 Telstra

21 Premier of Western Australia

22 Corruption and Crime Commission of Western Australia

23 Australian Federal Police

24 Attorney-General's Department

APPENDIX 2

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

Sydney, 15 March 2006

Law Council of Australia

Mr John North, President

Ms Pradeepa Jayawardena, Legal Policy Officer

Electronic Frontiers Australia

Ms Irene Graham, Executive Director

Australian Securities and Investment Commission

Ms Louise Macaulay, Director, Enforcement Policy and Practice

Mr Keith Inman, Director, Enforcement

Office of the Privacy Commissioner

Mr Timothy Pilgrim, Deputy Privacy Commissioner

Dr Hugh Clapin, Deputy Director, Policy

Gilbert + Tobin Centre for Public Law

Professor George Williams

Attorney-General's Department

Mr Geoff McDonald, Assistant Secretary, Security Law

Mr Cameron Gifford, Acting Principal Legal Officer, Security Law Branch

Ms Maree Hume, Acting Senior Legal Officer, Security Law Branch

Australian Federal Police

Federal Agent John Lawler, Deputy Commissioner

Federal Agent Andrew Colvin, Chief of Staff

Mr Peter Whowell, Manager, Legislation Program

NSW Council for Civil Liberties

Mr Cameron Murphy, President

Dr Richard Bibby, Assistant Secretary