Electronic Frontiers Australia Inc

PO Box 382 North Adelaide
SA 5006 AUSTRALIA
www.efa.org.au
email@efa.org.au
Tel: 07 3424 0201
Fax: 07 3424 0241

12 March 2006

Committee Secretary
Senate Legal and Constitutional Legislation Committee
Department of the Senate
Parliament House
Canberra ACT 2600

Via Email: legcon.sen@aph.gov.au

Dear Sir

Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006

Please find attached submission from Electronic Frontiers Australia Inc. to the Committee's inquiry.

Yours faithfully

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)
Submission

To: Senate Legal and Constitutional Legislation Committee
Re: Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006

12 March 2006

Contents:

1. Executive Summary

a. EFA generally supports the stored communications provisions. We consider, however, that some definitions may need amendment to ensure clarity of intent, that some aspects of the provisions relating to issue of warrants could be improved, and that the safeguards and accountability measures are not adequate.

b. EFA is concerned about whether a "stored communications warrant" will be necessary to access a stored *copy* of a communication, or whether the definitions leave a loophole that enables access to stored copies with "some other lawful authority" such as an ordinary search warrant. We recommend that amendments be made to ensure that copies of communications can not be accessed without a stored communications warrant.

c. It appears that, although a number of existing definitions in the Act are amended by the Bill as a result of the addition of the stored communications warrant provisions, not all relevant definitions are amended, and some may not have been adequately amended.

d. The Bill should be amended to require the affidavit accompanying an application for a stored communications warrant to set out the name of the person and details sufficient to identify the telecommunications services in relation to which access is sought, as is required in relation to named person interception warrants.

e. EFA considers that applicants for a stored communications warrant should be required to state in the affidavit accompanying the application that no such warrant has been issued within the last 3 days.

f. EFA strongly believes that stored communication warrants should only be able to be issued by (in addition to persons who may issue interception warrants) a Judge of a State/Territory Supreme Court.

g. EFA submits that the Bill should be amended to define "involvement in a contravention" in substantially the same way as the existing provisions defining "involvement in an offence".

h. EFA submits that issuers of stored communications warrants should be permitted to have regard to additional matters relevant to stored communications (concerning the extent of interference with privacy) such as the period during which communications occurred, and whether the stored communications are likely to include communications that are the subject of legal professional privilege.

i. We submit that definitional issues in relation to access to the Sent box of the person in respect of whom the warrant is issued need to be addressed and resolved to ensure that it is clear that communications "made by" such a person may be accessed when held/stored in connection with the telecommunications service provided to them, not by searching through mail received by/held for other persons who are not named in the warrant.

j. EFA's interpretation of the Bill is that the AFP will not be permitted to use a Crimes Act warrant to access remotely stored communications. However, if that interpretation is incorrect, then subsection 3LB of the Crimes Act should be amended to prohibit notification to telecommunications service providers in the foregoing circumstances.

k. Consideration should be given to means of ensuring/enforcing compliance with the safeguards and accountability measures by State/Territory enforcement agencies.

l. The Bill should be amended to prohibit disclosure and use of accessed information in relation to offences and contraventions with lower penalties than the stored communications warrant issuing threshold.

m. EFA considers that the reduced record keeping and inspection provisions combined with the proposed reduced reporting requirements result in inadequate safeguards and controls against misuse of covert access to stored communications by way of stored communications warrants. Accordingly, we submit that additional safeguards should be implemented.

n. The reporting requirements should be amended to substantially the same as requirements relating to named person interception warrants.

o. The Bill should be amended to delete, or specify the meaning of, the references to "renewal applications" in relation to stored communications warrants.

p. Individuals who have been the subject of covert surveillance by way of accessing their communications at a telecommunications service provider's premises should be notified of the details of that covert search/surveillance within 90 days of the cessation of the interception. If it is not to be required that individuals be notified, a Public Interest Monitor should be involved in the granting of warrants.

q. The Bill should be amended to include provisions amending Section 280 of the Telecommunications (Interception) Act 1979 to make clear than an enforcement agency as defined in Section 282 of that Act must provide a stored communications warrant in order to access stored communications.

r. If the stored communications are likely to include communications that are the subject of legal professional privilege, the communications sought to be seized should be required to be placed in the confidential safekeeping of an independent person and the relevant individual provided with the opportunity to prevent disclosure of any such communications to the agency.

s. EFA supports deletion of the outdated exception to the prohibition on interception, often referred to as the "participant monitoring" exception, which we understand some businesses and other organisations perceive as permitting them to covertly monitor and record incoming calls.

t. EFA strongly objects to the so−called "B−Party" provisions which vastly expand the circumstances in which, and the frequency with which, non−suspects' telecommunications services may be intercepted and monitored. It is of great concern that "B−Party" provisions could be used to intercept the telephone services of non−suspect persons who are, for example, lawyers or other persons who make and receive many calls that are subject to legal professional, or other, privilege. Furthermore, the Bill does not implement the controls suggested in the Blunn report in relation to innocent party interceptions. We recommend that "Schedule 2 − B−Party Interception" be deleted from the Bill.

u. EFA considers it highly inappropriate to permit equipment−based interception prior to the development of a "unique and indelible identifier of the source of telecommunications" as a basis for access. EFA is strongly opposed to warrants being issued based on "device numbers" that may identify multiple items of equipment, due to the potential for interception of communications sent to or from a device that is not used by the suspect but has the same number as another device that is used by the suspect. We recommend that "Schedule 3−Equipment−based interception" be deleted from the Bill.

▲ Go to Contents List

2. Introduction

01. Electronic Frontiers Australia Inc. ("EFA") appreciates the opportunity to make this submission to the Committee's Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006[1].

02. By way of background, we advise that in 2005 EFA sent a comprehensive submission to the Blunn Review[2] and the following extracts from the Executive Summary outline the key aspects of the EFA policy position submitted:

> "*The covert surveillance nature of search/seizure of individuals' communications at telecommunications service providers' premises is vastly more open to misuse and abuse than execution of a search warrant at an individual's own premises. Accordingly use of 'some other form of lawful authority, such as a search warrant' (something other than an interception warrant) at telecommunications service providers' premises to access content of communications should not be permitted unless markedly more appropriate safeguards and controls are put in place than currently exist.*"
>
> "*All communications that are being, or have been, carried over a telecommunications system should be afforded protection of the TI Act while they remain stored on a telecommunications service provider's equipment. We believe such a policy approach is the only means of providing certainty in relation to means of lawful access by government agencies and appropriate protection for the privacy of individuals who use the telecommunications system.*"
>
> "*A new type of warrant (e.g. a 'stored communications warrant') should be created for the specific purpose of authorising access to communications stored on a telecommunications service provider's equipment. Appropriate provisions regulating issue and use of a new warrant and related use and disclosure of seized communications should be inserted into the TI Act and access under authority of such a warrant made an exception to the prohibition on interception.*"

03. The *Telecommunications (Interception) Amendment Bill 2006*[3], in our analysis, implements a stored communications access regime which is generally similar to that recommended in our submission to the Blunn Review. Accordingly, we are pleased to be able to inform the Committee that EFA generally supports the stored communications provisions. We consider, however, that some definitions may need amendment to ensure clarity of intent, that some aspects of the provisions relating to issue of warrants could be improved, and that the safeguards and accountability measures are not adequate. This submission includes a number of recommendations for improvements.

04. EFA also supports deletion of the outdated exception to the prohibition on interception, often referred to as the "participant monitoring" exception, which we understand some businesses and other organisations perceive as permitting them to covertly monitor and record incoming calls.

05. EFA is strongly opposed to the innocent party ("B−Party") interception provisions. Schedule 2 should be deleted from the Bill.

06. EFA is also strongly opposed to the "equipment−based" interception provisions (which were **not** recommended in the Blunn Report[4]). In our view the provisions are technically incomprehensible. It is not apparent how they could or would operate in practice, and we doubt that any current telecommunications devices are uniquely identifiable by a number that can be used for the purpose of identifying and capturing real−time communications being made to and from a particular device and only that device. In our analysis, the primary purpose is probably to enable interception of communications to and from B−Party equipment such as modems and computers. If that is not the purpose, then a major overhaul of the definitions and provisions in "Schedule 3−Equipment−based interception" needs to be undertaken to make clear what is

intended. Any such amendments should be made the subject of a separate Parliamentary inquiry at some future time. Schedule 3 should be deleted from the Bill.

▲ Go to Contents List

3. Stored Communications

3.1 Definitions

3.1.1 Definition of "stored communication"

07. EFA agrees generally with the apparent intent of the definition of a "stored communication". However, 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. Hence it is not clear what type of lawful authority would apply to access to such records by enforcement agencies. We discuss the relevant definitions and provide examples of relevant circumstances below.

08. The Bill states:

> "***stored communication*** *means a communication that:*
> *(a) has passed over a telecommunications system; and*
> *(b) is not passing over that or any other telecommunications system; and*
> *(c) is held on equipment that is operated by, and is in the possession of, a carrier [which includes a carriage service provider/Internet service provider]; and*
> *(d) is accessible to the intended recipient of the communication.*"

09. The existing Act (*Telecommunications (Interception) Act 1979*[5]) states:

> "***communication*** *includes conversation and a message, and any part of a conversation or message, whether:*
> *(a) in the form of:*
> *(i) speech, music or other sounds;*
> *(ii) data;*
> *(iii) text;*
> *(iv) visual images, whether or not animated; or*
> *(v) signals; or*
> *(b) in any other form or in any combination of forms.*"

10. The above definitions leave open to question whether or not a *copy* of a communication (e.g. an email or SMS message) is also a "communication" and hence whether a stored *copy* of a communication is a "stored communication" as defined. This issue does not arise in the context of interception of telephone calls because records/copies of telephone calls do not automatically come into existence and making a record/copy is of itself an interception.

11. EFA's concern in this regard is whether a "stored communications warrant" will be necessary to access a stored *copy* of a communication, or whether the definitions leave a loophole that enables access to stored copies with "some other lawful authority" such as an ordinary search warrant.

12. There are at least two types of records of communications that may be stored on carriers' equipment in relation to which the above issue arises:

a. Copies of communications stored in a sender's "Sent" box/folder on a carrier's equipment. For example, when an email message is sent, a copy of that communication may be automatically created and stored in the sender's "Sent" folder/box on an ISP's equipment if the sender is using e.g. web based email or IMAP (and the sender has not intentionally configured the software to not create and retain a copy).
b. Copies of communications stored on a carrier's backup devices/tapes for the purpose of disaster recovery.

13. If the above are regarded as *copies* of communications, *not* "communications", then it appears they cannot be "stored communications" and therefore access to same could not be authorised by a stored communications warrant. This raises the question of whether such records of communications could be accessed by "some other lawful authority" such as an ordinary search warrant.

14. If, on the other hand, copies are regarded as "communications", it nevertheless appears the records referred to in item (a) above would not be accessible with authority of a stored communications warrant because they do not meet the definition of "stored communications" because they are not accessible to the intended recipient. In this regard the Bill states:

> "***accessible**, in relation to a communication, has the meaning given by section 5H":*
>
> > *"5H When a communication is accessible to the intended recipient*
> > *(1) For the purposes of this Act, a communication is accessible to its intended recipient if it:*
> > *(a) has been received by the telecommunications service provided to the intended recipient; or*
> > *(b) is under the control of the intended recipient; or*
> > *(c) has been delivered to the telecommunications service provided to the intended recipient.*
> > *(2) Subsection (1) does not limit the circumstances in which a communication may be taken to be accessible to its intended recipient for the purposes of this Act.*"

15. Communications stored in a sender's "Sent" box/folder are not "under the control of the intended recipient", and the sender's carrier has no means of knowing whether or not the communication has been delivered to, or received by, the telecommunications service provided to the intended recipient by some other carrier. In addition, it seems doubtful that a copy of communication stored in a Sent box can be regarded as "a communication that...has passed over a telecommunications system". In our view it is a copy of a communication that (possibly) did. Again, these aspects give rise to the question of whether communications stored in a sender's Sent box may be able to be accessed by "some other lawful authority" such as an ordinary search warrant, on claimed grounds that they are not "stored communications". This issue is further addressed in the section "What stored communications warrants authorise" later herein.

16. In relation to item (b) above, i.e. copies of communications stored on a carrier's backup devices/tapes, if copies are regarded as "communications" then it appears these may be legislatively regarded as accessible to the intended recipient, assuming the backup was of the content of the carrier's customers' mail boxes because communications in those mail boxes are to be legislatively regarded as "ha[ving] been delivered to the telecommunications service provided to the intended recipient".

17. EFA submits that amendments should be made to ensure that copies of communications can not be accessed without a stored communications warrant. We consider an appropriate amendment might be to amend the definition of "communication" to state that for the purposes of Chapter 3 (Access to Stored Communications) it includes a copy of a communication. An alternative possibility, of amending the definition of "stored communication" to, for example, state that it includes a copy of a stored communication, seems problematic due to the fact that the (original) communication may no longer be a "stored

communication". For example, it has been downloaded and deleted from the recipient's mail box, but a copy still exists on a backup tape. Hence it is difficult to see how legislation could apply to something described as a "copy" of something that does not exist. We therefore consider amending the definition of "communication" may be the best approach.

18. It should be noted that during the short period since this complex Bill was tabled, we have not had sufficient time to fully analyse the possible effects of the suggested amendment above to ensure the desired result would be achieved and that there would be no unintended consequences.

Recommendation:

That amendments be made to ensure that copies of communications can not be accessed without a stored communications warrant.

▲ Go to Contents List

3.1.2 Definition of accessing a stored communication and "record"

19. We note that the Explanatory Memorandum[6] states that the definition of accessing a stored communication "is based on the definition of intercepting a communication in section 6 of the Act" and the two relevant definitions are:

> "*6 Interception of a communication*
> *(1) For the purposes of this Act, but subject to this section, interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.*"

> "*6AA Accessing a stored communication*
> *For the purposes of this Act, accessing a stored communication consists of listening to, reading or recording such a communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication.*"

20. Both the above definitions refer to "recording" a communication which is defined in the existing Act as follows:

> "*record means:*
> *(a) in relation to information−a record or copy, whether in writing or otherwise, of the whole or a part of the information; or*
> *(b)* ***in relation to an interception****, whether or not in contravention of subsection 7(1), of a communication:*
> *(i) a record or copy, whether in writing or otherwise, of the whole or a part of the communication, being a record or copy made by means of the interception; or*
> *(ii) a record or copy, whether in writing or otherwise, of the whole or a part of a record or copy that is, by virtue of any other application or applications of this definition, a record obtained by the interception.*" (emphasis added)

21. EFA considers the definition of record should be amended so that it applies in relation to, not only an interception, but also accessing a stored communication.

Recommendation:

That the definition of "record" be amended by insertion of the following new clause:

> (c) in relation to accessing a stored communication, whether or not in contravention of subsection 108(1):
> (i) a record or copy, whether in writing or otherwise, of the whole or a part of the communication, being a record or copy made by means of accessing a stored communication; or
> (ii) a record or copy, whether in writing or otherwise, of the whole or a part of a record or copy that is, by virtue of any other application or applications of this definition, a record obtained by accessing a stored communication.

▲ Go to Contents List

3.1.3 Existing definitions that appear to require amendment

22. A number of existing definitions in the Act are amended by the Bill as a result of the addition of the stored communications warrant provisions. However, it appears to us that not all relevant definitions are amended by the Bill, and in the case of those that are, some may not have been adequately amended.

23. For example, Section 6H "Person to whom application relates" is being amended to include reference to applications for stored communications warrants. However, the result of the amendment appears to be that s6H would only apply to an application for a stored communications warrant made by an agency to a Judge or nominated AAT member, and not to application made to a "magistrate". It is not readily apparent to us why this difference would exist, however, due to the short time frame since the Bill was tabled, we have not had sufficient time to analyse whether or not there is a legitimate reason for the difference.

24. Another existing provision which it appears should be amended, or equivalent provisions inserted in relation to stored communications warrants, is the definition of "communicating" in Section 5A−Communicating etc. certain information.

25. While the above came to our notice while analysing the Bill, we have not specifically checked whether or not there are other existing definitions etc that may need updating.

▲ Go to Contents List

3.2 Stored Communications Warrants (Part 3−3)

3.2.1 Applications for stored communications warrants (Div 1)

3.2.1(a) Lack of identification of person and telecommunications service/s

26. The Bill (Part 3−3, Div 1) states:

> "*110(1) An enforcement agency may apply to an issuing authority for a stored communications warrant* ***in respect of a person***." (emphasis added)

27. As noted in the Explanatory Memorandum, stored communications warrants are more similar to named person interception warrants than to telecommunications service interception warrants:

> "*New section 110 provides that an agency may apply for a warrant authorising access to stored communications in respect of a person. This means that stored communications are*

more similar to named person interception warrants than service interception warrants, in that a stored communications warrant may authorise access to stored communications in relation to more than one telecommunications service. For example, a stored communications warrant may authorise access to all SMS messages sent to and from a specified mobile telephone number and all emails sent to and from a specified email address."

28. However, unlike the requirements pertaining to named person interception warrants, the Bill does require that an application for a stored communications warrant, or the warrant itself, specify the mobile number/s or email address/es etc in relation to which access is authorised by the warrant.

29. Proposed s113 concerning stored communications warrants states:

"*113 Affidavits to accompany written applications*
(1) The application must, if it is in writing, be accompanied by an affidavit complying with this section.
(2) The affidavit must set out the facts and other grounds on which the application is based."

30. In contrast, existing s42 concerning interception warrants states:

"*42 Affidavit to accompany written application*
(1) A written application by an agency for a warrant shall be accompanied by an affidavit complying with this section.
(2) The affidavit shall set out the facts and other grounds on which the application is based.
(3) The affidavit shall specify the period for which it is requested that the warrant be in force and shall state why it is considered necessary for the warrant to be in force for that period.
(4) If the application is for a ***telecommunications service warrant****, the affidavit shall set out, in relation to the service, and in relation to each person to whom the application relates, the following information, so far as it can be derived from the agency's records:*

(a) the number of previous applications (if any) for warrants that the agency has made and that related to the service or to that person, as the case may be;
(b) the number of warrants (if any) previously issued on such applications; and
(c) particulars of the use made by the agency of information obtained by interceptions under such warrants.

(4A) *If the application is for a* ***named person warrant****, the affidavit must set out:*

(a) the ***name or names by which the person is known****; and*
(b) ***details (to the extent these are known to the chief officer) sufficient to identify the telecommunications services the person is using, or is likely to use****; and*
(c) the number of previous applications (if any) for warrants that the agency has made and that related to the person or to a service that the person has used; and
(d) the number of warrants (if any) previously issued on such applications; and
(e) particulars of the use made by the agency of information obtained by interceptions under such warrants." (emphasis added)

31. EFA submits that the Bill should be amended to require the affidavit accompanying an application for a stored communications warrant to set out the name of the person and details sufficient to identify the

telecommunications services in relation to which access is sought, as is required by s42(4A)(a) and (b) above in relation to named person interception warrants. We note that proposed s6EB appears to assume that a stored communications warrant would contain information identifying the person and also identifying the relevant telecommunications services:

> "*6EB Stored communications warrant information*
> *A reference in this Act to stored communications warrant information is a reference to:*
> *(a)...; or*
> *(b) any other information that is likely to enable the identification of:*
> *(i)* ***the telecommunications service to which a stored communications warrant relates; or***
> ***(ii) a person specified in a stored communications warrant as a person using or likely to use the telecommunications service to which the warrant relates.***" (emphasis added)

32. However, it is not apparent from the Bill how the issuing authority would obtain such information − perhaps verbally from the applicant? We consider that applicants for stored communications warrants should be clearly required to include such information in an affidavit accompanying the application.

3.2.1(b) No requirement to provide information about previous stored communications warrants

33. EFA also considers that information substantially the same as that required by existing s42(4A)(c) to (e) inclusive should also be required to be included in affidavits accompanying applications for stored communications warrants. In this regard, we note that proposed s119 states:

> "*(3) An issuing authority must not vary a stored communications warrant by extending the period for which it is to be in force.*
> *(4) This section does not prevent the issue of a further warrant in respect of the person in respect of whom the warrant was issued.*
> *(5) However, if the further warrant relates to the same telecommunications service as the previous warrant, it must not be issued within 3 days after the day on which the previous warrant was executed or (if subsection (2) applies) was last executed.*"

and the Explanatory Memorandum states in relation to ss(5) above that "*[t]his time limit is to ensure that agencies are not able to get a new stored communications warrant daily, which would undermine the separate interception warrant regime*".

34. However, it appears that an issuing authority may not know that a warrant relating to the same telecommunications service had been issued during the past three days because there is no requirement that the applicant inform the issuing authority in that regard. EFA considers that applicants should be required to state in the affidavit accompanying the application that no such warrant has been issued within the last 3 days.

Recommendation:

That a new subsection be inserted into proposed s113 to require that affidavits accompanying applications for stored communications warrants set out the same information as in existing s42(4A)(a) to (e) inclusive, but that (d) include date information in relation to the most recent warrant issued and (e) be rephrased to refer to 'access under' instead of 'interceptions under', as follows:

> 113 (2A) The affidavit must also set out:
>
> > (a) the name or names by which the person is known; and
> > (b) details (to the extent these are known to the chief officer) sufficient to identify the telecommunications services the person is using, or is likely

to use; and
(c) the number of previous applications (if any) for warrants that the agency has made and that related to the person or to a service that the person has used; and
(d) the number of warrants (if any) previously issued on such applications and the date on which the most recent warrant was issued; and
(e) particulars of the use made by the agency of information obtained by access under such warrants.

Go to Contents List

3.2.2 Issuing of stored communications warrants (Div 2)

3.2.2(a) Issuing Authorities

35. We observe that stored communications will be able to be issued by "a magistrate" appointed by the Minister for that purpose, as well as by persons who are able to issue interception warrants (i.e. a judge of a court created by the Parliament, or a Federal Magistrate, or a member of the AAT, who has been appointed by the Minister for that purpose) (Section 6DB).

36. EFA recognises that there would be a need to provide for a greater number of persons able to issue stored communications warrants, due to the larger number of agencies that will be able to apply for such warrants, and that would be why "a magistrate" has been included.

37. However, as stated in our submission to the Blunn Review, EFA is of the strongly held view that stored communication warrants should only be able to be issued by (in addition to persons who may issue interception warrants) a Judge of a State/Territory Supreme Court.

Recommendation:

That issuing authorities for stored communications warrants be limited to persons authorised to issue interception warrants and Judges of a State/Territory Supreme Court.

Go to Contents List

3.2.2(b) Definition of "involvement in" contraventions

38. In relation to issuing of stored communications warrants, the Bill refers to "a serious contravention in which the person is involved" (s116(1)) and defines "serious contravention" to include serious offences (existing Class 1 and 2 offences), plus other criminal offences and pecuniary penalty offences. However, unlike the equivalent provisions relating to involvement in "serious offences" and associated issue of interception warrants, the Bill does not define the meaning of "involved in" a serious contravention in relation to issue of stored communication warrants.

39. The Bill states:

> "*116 (1) An issuing authority to whom an enforcement agency has applied for a stored communications warrant* ***in respect of a person*** *may, in his or her discretion, issue such a warrant if satisfied, on the basis of the information given to him or her under this Part in connection with the application, that:*
> ...

(d) information that would be likely to be obtained by accessing those stored communications under a stored communications warrant would be likely to assist in connection with the investigation by the agency of ***a serious contravention in which the person is involved****; and"* (emphasis added)

40. and the equivalent existing provision in relation to interception warrants states:

"*46A (1) Where an agency applies to an eligible Judge or nominated AAT member for a warrant* ***in respect of a person*** *and the Judge or nominated AAT member is satisfied, on the basis of the information given to the Judge or nominated AAT member under this Part in connection with the application, that:*
...
(d) information that would be likely to be obtained by intercepting under a warrant communications made to or from any telecommunications service that the person is using, or is likely to use, would be likely to assist in connection with the investigation by the agency ***of a*** ~~*class 2*~~ ***serious offence, or*** ~~*class 2*~~ ***serious offences, in which the person is involved****; and*" (emphasis added)

41. In relation to interception warrants and s46A(1)(d) above, the Act states:

"*6B Involvement in an offence*
For the purposes of this Act, a person shall be taken to be involved in an offence if, and only if, the person:
(a) has committed, or is committing, the offence; or
(b) is suspected on reasonable grounds of having committed, of committing, or of being likely to commit, the offence."

42. EFA submits that the Bill should be amended to define "involvement in a contravention" in substantially the same way as the existing provisions (s6B above) defining "involvement in an offence".

Recommendation:

That the Bill be amended to include a new subsection, similar to existing s6B, as follows:

Involvement in a contravention
For the purposes of this Act, a person shall be taken to be involved in a contravention if, and only if, the person:
(a) has committed, or is committing, the contravention; or
(b) is suspected on reasonable grounds of having committed, of committing, or of being likely to commit, the contravention.

▲ Go to Contents List

3.2.2(c) Matters to which the issuing authority must have regard

43. We note that the matters to which an issuing authority must have regard (s116(2)) appear to be the same as applicable to the issue of interception warrants, that is, other than phrasing changes relevant to access as distinct from interception.

44. While EFA supports the above approach, we consider that an issuing authority should also be permitted to take additional matters relevant to stored communications into account:

- in relation to how much the privacy of any person or persons would be likely to be interfered with by accessing the stored communications:
    - ♦ the fact that the stored communications may include communications that have been sent, received and stored over a much longer period than the maximum initial duration of an interception warrant (i.e. over a much longer period than 90 days, including possibly years);
    - ♦ whether the communications or documents sought can be identified or described with sufficient particularity, whether by date range, or the content of e.g. 'To' and 'From' fields in email messages, or any other means, in order to minimise the privacy intrusion involved in accessing/seizing communications that may have been stored over many months or years;
- whether the stored communications are likely to include communications the subject of legal professional privilege, and if so whether communications sought to be seized should be placed in the confidential safekeeping of an independent person and the relevant individual provided with the opportunity to prevent disclosure of any such communications to the agency, by way of liaison with the agency and if that fails by application to the issuer of the warrant;

45. and that in relation to any of the above matters the issuing authority may include warrant conditions limiting access to stored communications.

Recommendation:

That issuers of stored communications warrants be permitted to have regard to additional matters relevant to stored communications as outlined above.

▲ Go to Contents List

3.2.3 What stored communications warrants authorise

46. The Bill states:

> "*117 What stored communications warrants authorise*
> *A stored communications warrant authorises persons approved under subsection 127(2) in respect of the warrant to access, subject to any conditions or restrictions that are specified in the warrant, a stored communication:*
> *(a) that was made by the person in respect of whom the warrant was issued; or*
> *(b) that another person has made and for which the intended recipient is the person in respect of whom the warrant was issued;*
> *and that becomes, or became, a stored communication before the warrant is first executed in relation to the carrier that holds the communication.*"

47. In EFA's view, there appears to be definitional issues in relation to the proposition in s117(a) above that a stored communications warrant authorises access to a stored communication made by the person in respect of whom the warrant was issued. For example, in relation to email, generally speaking communications made by such a person would only be held on a carrier's equipment in one of two places:
a) in the "Sent" box/folders of the sender, i.e. the person in respect of whom the warrant was issued, or
b) in the (incoming) mailbox/folders of the recipient.

48. As discussed in Section 3.1.1 above (Definition of "stored communication"), it appears that the contents of the "Sent" box/folder of the person in respect of whom the warrant is issued are not "stored communications" as defined in the Bill either because the contents may be regarded as copies not "communications" and/or because the contents are not "accessible to the intended recipient[s]" as defined.

49. This situation raises the question of whether the proposed legislation intends (without making it clear) that it will merely be assumed that a copy of a communication stored in a sender's Sent box is a "communication" and has in fact been delivered to/received by the intended recipient's telecommunications service, or whether it is intended that a warrant issued "in respect of a person" may require a carrier to engage in a fishing trip through **other** person's mailboxes looking for communications "made by" (sent by/received from) the person in respect of whom the warrant was issued.

50. The latter scenario appears to be contrary to the apparent intent of the proposed legislation and we therefore assume it is not the intent. However we submit that definitional issues in relation to access to the Sent box of the person in respect of whom the warrant is issued need to be addressed and resolved to ensure that it is clear that communications "made by" such a person may be accessed when held/stored in connection with the telecommunications service provided to them, not by searching through mail received by/held for other persons who are not named in the warrant.

Recommendation:

That the Bill be amended to make clear that a stored communications warrant authorises access to communications, and copies of communications, that have been sent by the person in respect of whom the warrant is issued, when those communications/copies are stored in connection with the sender's telecommunications service, whether or not those communications/copies are accessible to the intended recipient.

▲ Go to Contents List

3.2.4 Remote Access to Stored Communications

51. As the Committee is aware, a principle reason for enactment of the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* ("TIA(SC) Act") was to resolve the issue of whether or not the Australian Federal Police ("AFP") could lawfully use a Crimes Act Part 1AA search warrant, while at a suspect's premises, to access/download email stored remotely on an ISP's mail server, or whether an interception warrant was necessary. The C'th Director of Public Prosecutions was of the opinion that Section 3L of the Crimes Act provided authority, while the Solicitor−General was of the opinion that an interception warrant was necessary. The effect of the TIA(SC) Act was to permit the AFP to access communications stored remotely with a Crimes Act warrant.

52. On our reading of the current Bill, after it commences operation, remote access (i.e. use of the telecommunications system to obtain access from a remote location) to communications stored on a carrier's equipment will not be permitted with a Crimes Act warrant. In this regard, we note that while Section 108 includes an exception to the prohibition on access applicable to "(c) accessing a stored communication under a computer access warrant issued under section 25A of the *Australian Security Intelligence Organisation Act 1979*", there is no exception referring to search warrants issued under the C'th Crimes Act.

53. We observe that the note to Section 108(1) states:

> "*Note: This section does not prohibit accessing of communications, that are no longer passing over a telecommunications system, from the intended recipient or from a telecommunications device in the possession of the intended recipient.*"

54. We understand the use of the word "from" in the above refers to obtaining access to communications from the telecommunications device, i.e. that are stored on that device, not using that device to obtain access to communications from somewhere else, i.e. that are stored somewhere else, such as by finding (on the device), or guessing, a suspect's password and covertly logging into their email box on an ISP's equipment. We assume that the purpose of the note is to seek to make clear that if, for example, the AFP is executing a

Crimes Act warrant at a person's home and email messages are automatically being delivered to the suspect's computer there is no prohibition on the AFP reading those messages stored on the suspect's computer. Similarly if a law enforcement agency lawfully seizes a mobile phone, and SMS messages are automatically delivered to it when it is switched on, there is no prohibition on the reading of those messages stored on the mobile phone.

55. EFA's support for the stored communications warrant provisions and related definitions is premised on the assumption that the above interpretation is correct. It would be inappropriate to permit remote access by use of a Crimes Act warrant because such warrants may be issued in relation to investigation of suspected offences that do not meet the threshold for issue of a stored communications warrant.

56. However, if the above interpretation is not correct (that is, if the AFP will be permitted to use Crimes Act warrants to access remotely stored communications) then the Bill must be amended to include provisions amending subsection 3LB of the Crimes Act so that the AFP will not be required to notify an ISP of the fact that a search warrant has been executed at one of the ISP's customer's homes or other premises.

57. Such amendments would be essential to protect the right of individuals whose premises are searched not to have personal, or any other, information about them unnecessarily disclosed to third parties (i.e. carriers) by law enforcement agencies.

58. In this regard, subsection 3LB[7] states that if "data that is held on premises other than the warrant premises is accessed under subsection 3L(1)[8]" the executing officer must "notify the occupier of the other premises that the data has been accessed under a warrant" as soon as it is "practicable" to do so.

59. EFA considers s3LB demonstrates that s3L was not intended to authorise remotely accessing "data" that consists of a suspect's (or anyone else's) private communications stored on a telecommunication's service provider's system. It is totally inappropriate for police to disclose to a telecommunications service provider that they have remotely accessed a customer's email under warrant executed at the customer's premises. This type of information about a customer should not be disclosed to the service provider; it is none of the service provider's business.

60. Hence, if our interpretation of the Bill is incorrect (that is, if the AFP will be permitted to use Crimes Act warrants to access remotely stored communications) then subsection 3LB of the Crimes Act must be amended to prohibit notification to telecommunications service providers in the above circumstances.

▲ Go to Contents List

3.3 Safeguards and Accountability Measures

3.3.1 Enforceability in relation to State/Territory enforcement agencies

61. EFA observes that the Bill contains provisions intended to regulate the use, communication and recording of information obtained by accessing stored communications, and require enforcement agencies to report to the Minister regarding the use of stored communications powers.

62. However, it is not clear how, if at all, the Commonwealth could enforce these provisions in the event that a State/Territory enforcement agency fails to comply with same. For example, if a State agency chooses not to destroy accessed information that is not likely to be required for a purpose referred to in proposed subsection 139(2), or uses accessed information in non−permitted (State/Territory) proceedings, etc, what action could be taken by the Commonwealth to make such an agency comply?

63. In the case of intercepted 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 (see Section 35−Preconditions for Declaration). As stated in the Sherman *Report of Review of Named Person Warrants and Other Matters*[9]:

> "*32. The legal foundation for TI legislation is contained in section 51 of the Constitution which, so far as is relevant, provides in placitum (v) that the Commonwealth Parliament has the power to make laws for the peace, order and good government of the Commonwealth with respect to:*
> *"postal, telegraphic, telephonic, and other like services."*
> *33. This is an important point because the States and Territories only acquire the power to intercept telecommunications through Commonwealth law, and they exercise that power subject to conditions imposed by the Interception Act.* ***It is necessary however for some aspects of the process to be regulated by State and Territory laws****, ...*
> *...*
> *41. The Interception Act (and supplementary State laws) authorise lawful TI and the conditions for its use. Commonwealth agencies − the AFP, the Australian Crime Commission (ACC) and ASIO − are authorised directly by the Interception Act.* ***State agencies are similarly authorised by the Interception Act but in their case the record keeping, reporting and inspecting functions are regulated by State law.***
> *42. Part VI, Division 2 of the Interception Act provides for the declaration of State law enforcement agencies as agencies for the purposes of the Interception Act.* ***State agencies can only be declared when the relevant State complies with a number of preconditions for declaration which are set out in section 35 of the Interception Act. These conditions relate to the keeping of records, providing copies of warrants, as well as making effectiveness and other reports on TI operations.[10] [10. These pre−conditions are implemented by State legislation.]*** *...*
> *43. Section 35 also requires regular inspection of eligible authority records by an inspecting authority (usually the State Ombudsman11) in a manner similar to the Commonwealth Ombudsman's role under the Interception Act in relation to Commonwealth agencies other than ASIO. In relation to ASIO, the inspection role is carried out by the Inspector General of Intelligence and Security (IGIS). ...*" (emphasis added)

64. 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.

65. EFA respectfully suggests that the Committee may wish to inquire into whether or not the Commonwealth has adequate powers to ensure that State/Territory agencies comply with the provisions concerning concerning use, communication and recording of information obtained by accessing stored communications, and related reporting requirements.

66. It appears to us that the only option the Commonwealth would have if an agency did not comply, and a State/Territory Government declined to make their agency comply, would be to amend the Act to exclude the particular agency from being permitted to obtain stored communication warrants. This would generally speaking not be able to be done in a timely manner.

67. EFA suggests that consideration be given to amending the definition of enforcement agency in the Bill, which currently states:

> "*enforcement agency has the same meaning as in section 282 of the Telecommunications Act 1997, and includes an interception agency and an eligible authority of a State.*"

to exclude an agency specified in the TI Regulations from being able to obtain stored communications

warrants and grant the Minister power to specify in the TI Regulations any agency that fails to comply with the provisions referred to above (i.e. Parts 3−4, 3−5, or 3−6).

Recommendation:

That consideration be given to means of ensuring/enforcing compliance with the safeguards and accountability measures by State/Territory enforcement agencies.

▲ Go to Contents List

3.3.2 Dealing with accessed information etc. (Part 3−4)

68. We observe that proposed Part 3−4 ("Dealing with accessed information etc.") appears to be generally similar to the existing provisions concerning intercepted information insofar as those provisions are relevant to accessed information (although as discussed in the foregoing section, it is not clear how, if at all, these provisions can be enforced if a State/Territory agency does not comply).

69. However, EFA is 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 issued.

70. The threshold for issue of a stored communications warrant is:

- offences punishable by a maximum period of at least 3 years or a fine of at least 180 penalty units for individuals (900 penalty units for corporations); or
- civil contraventions with a pecuniary penalty of at least 180 penalty units for individuals (900 penalty units for corporations).

71. A much lower threshold is set for use and disclosure of accessed information. Proposed section 139 creates an exception to the general prohibition on dealing with accessed information to enable enforcement agencies to communicate, use or record accessed information in relation to:

- offences punishable by a maximum period of at least 12 months or by a maximum fine of at least 60 penalty units (300 penalty units for corporations); and
- civil contraventions with a pecuniary penalty of at least 60 units (300 penalty units for corporations).

72. We acknowledge that in relation to interception warrants, while the imprisonment penalty threshold for issuing a warrant is generally 7 years, intercepted information is permitted to be used in relation to offences involving the lower penalty of at least 3 years imprisonment.

73. As the threshold for issuing stored communications warrants is itself 3 years imprisonment or 180 (900) penalty units, we question the justification for allowing accessed information to be used in relation to offences and civil contraventions involving lower penalties than the warrant issuing threshold.

74. Moreover, we note that the *Surveillance Devices Act 2005* enables warrants to be issued in relation to offences punishable by a maximum term of imprisonment of 3 years and offences against specified sections of the *Financial Transaction Reports Act 1988* and the *Fisheries Management Act 1991*, but does not permit any information obtained from the use of a warrant to be used in relation to offences involving lower penalties than the warrant issuing threshold.

Recommendation:

That the Bill be amended to prohibit disclosure and use of accessed information in relation to offences and contraventions with lower penalties than the stored communications warrant issuing threshold.

▲ Go to Contents List

3.3.3 Keeping and inspection of access records (Part 3−5)

75. We note that the provisions concerning inspection of access records by the C'th Ombudsman appear to be similar to those applicable to interception warrants, insofar as any similar records are required to be kept, although it is not clear what, if any, action the C'th Ombudsman can take to make State/Territory agencies provide relevant information and/or permit inspections in the event an agency declines to do so.

76. However, we also note that the record keeping requirements in relation to stored communications warrants are substantially less than those applicable to interception warrants. Among numerous other things, there is no requirement that a General Register of Warrants, or a Special Register of Warrants (containing details of warrants which do not lead, directly or indirectly, to a prosecution), be kept and inspected by the Minister.

77. EFA considers that the reduced record keeping and inspection provisions combined with the proposed reduced reporting requirements (as discussed in Section 3.3.4 below) result in inadequate safeguards and controls against misuse of covert access to stored communications by way of stored communications warrants. Accordingly, we submit that additional safeguards should be implemented as outlined in Section 3.3.5 later herein.

▲ Go to Contents List

3.3.4 Reports about access to stored communications (Part 3−6)

3.3.4(a) Reporting requirements

78. The proposed reporting requirements for stored communication warrants place markedly less obligations on enforcement agencies than applies in relation to interception warrants. In this regard the Explanatory Memorandum states:

> "*Reflecting the wider agency access and the lower [penalty] threshold to be met, the reporting requirements for stored communications warrant are not as burdensome on the agencies as the requirements for interception. Reduced reporting requirements are also consistent with general search warrants provisions.*"

79. EFA considers the threshold is irrelevant to reporting requirements. 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. It is very likely there will be vastly more stored communications warrants issued because these will be available in relation to a vastly greater number of offences and contraventions by a markedly greater number of Commonwealth and State/Territory criminal **and** civil enforcement agencies. Hence the communications of many more innocent parties (who have been in contact with a suspect at some time in the past) will be accessed.

80. EFA submits that the reporting requirements should be amended to become substantially the same as requirements relating to named person interception warrants, as outlined below.

81. Section 162 of the Bill states:

> "*162 Report to set out how many applications made and warrants issued*
> *(1) The report must set out, for each enforcement agency:*
> *(a) the relevant statistics about applications for stored communications warrants that the agency made during that year; and*
> *(b) the relevant statistics about telephone applications for stored communications warrants that the agency made during that year.*
> *(2) The report must set out:*
> *(a) the relevant statistics about applications for stored communications warrants that were made during that year; and*
> *(b) the relevant statistics about telephone applications for stored communications warrants that were made during that year; and*
> *(c) the relevant statistics about renewal applications made during that year; and*
> *(d) how many stored communications warrants issued on applications made during that year specified conditions or restrictions relating to access to stored communications under the warrants.*"

82. With regard to the above provisions, we submit that:

i. Subsection 2(d) should also be inserted into Subsection 1 so that the report will show **for each enforcement agency** how many warrants specified conditions or restrictions, as is required in reports about interception warrants (see Section 100).
ii. Subsection 2(c) should be deleted if our interpretation of relevant provisions is correct, as set out in Section 3.3.4(b) − "Reporting of (non−existent) renewal applications" below. (If our interpretation is not correct, then Subsection 2(c) should also be inserted in Subsection 1).
iii. New clauses should be added to both Subsections (1) and (2) requiring reporting on the number of stored communications warrants which involved accessing of telecommunications services in the following ranges − one service, 2−5 services, 6−10 services and more than 10 services, as is required in reports about named person interception warrants (see Section 100). Those reporting provisions resulted from the recommendation in the Sherman Report and we consider similar reporting should be required for the same reasons. Like named person warrants, a stored communication warrant may authorise/result in access to a significant number of services, which would mean the Bill's proposed statistical reporting provisions would provide no indication of the number of services being accessed in the Australian community and may be misleading in that regard.
iv. New clauses should be added to both Subsections (1) and (2) requiring reporting on the categories of offences/contraventions in relation to which applications for warrants were made (similar to Section 100(1)(f) and (g) and (2)(f) and (g) re interception warrants). Further comment in relation to specification of categories is provided below.

83. Section 163 of the Bill states:

> "*163 Report to contain information about effectiveness of warrants*
> *The report must set out, for each enforcement agency:*
> *(a) how many arrests were made during that year on the basis of information that was, or included, lawfully accessed information; and*
> *(b) how many proceedings ended during that year that were proceedings in which, according to the records of the agency, lawfully accessed information was given in evidence.*"

84. We note that, unlike reporting on interception warrants, s163 above does not require reporting on the number of convictions that were recorded, nor specification of the categories of offences/contraventions in relation to which stored communications warrants were issued. In contrast, reports on interception warrants are required to contain the following information:

"*102 Report to contain information about effectiveness of warrants*
(1) The report shall set out, for each Commonwealth agency, for each eligible Commonwealth authority, and for each eligible authority of a State:
(a) how many arrests were made during that year:
(i) in connection with the performance by the agency or authority of its functions; and
(ii) on the basis of information that was or included lawfully obtained information;
(b) ***the categories of the prescribed offences proceedings*** *by way of prosecutions for which ended during that year, being proceedings in which, according to the records of the agency or authority, lawfully obtained information was given in evidence; and*
(c) ***in relation to each of those categories:***
(i) the number of such offences in that category; and
(ii) the number of such offences in that category in respect of which convictions were recorded." (emphasis added)

85. EFA submits that s163 should be amended to require reporting on the number of convictions recorded and provide information concerning the categories of offences and contraventions.

86. However, as it is likely there would be vastly more offences/contraventions potentially needing to be specified than in relation to interception warrants (due to the lower penalty threshold and larger number of agencies) and the Bill does not place such offences/contraventions in categories, we consider categories for the purpose of reporting could be defined in a manner similar to the below:

- in the case of warrants issued in relation to "serious offences" (as defined in the Bill), the same categories as already specified for interception warrants;
- in the case of warrants issued in relation to offences carrying a penalty of imprisonment (that are not also "serious offences"), categories specified by number of years imprisonment, e.g. minimum 3 years, minimum 4 years, etc;
- in the case of warrants issued in relation to civil contraventions involving a pecuniary penalty, categories defined by range of penalty units.

87. EFA is of the firmly held view that the above level of detail should be provided. However, if that is not to be done, at the very least reports should be required to distinguish between warrants issued in relation to serious offences, other criminal offences and civil contraventions. EFA considers it important that the Minister, the Parliament and the public be provided with information that enables monitoring of the quantity and usefulness of warrants enabling access to information that could not previously be obtained (prior to December 2004) by the numerous Commonwealth, State and Territory criminal and civil enforcement agencies that were not able to obtain interception warrants. (We note that Telstra informed the Committee inquiry in June 2004[10] that "Telstra's practice has been to disclose stored communications in accordance with an interception warrant").

Recommendation:

That the reporting requirements be amended to substantially the same as requirements relating to named person interception warrants.

3.3.4(b) Reporting of (non−existent) renewal applications

88. We observe that proposed Section 162(2) requires a report concerning stored communication warrants to set out, among other things, "*(c) the relevant statistics about renewal applications made during that year*". However, on our reading of Section 119, there should not be any renewal applications because stored communications warrants will not be permitted to be renewed.

89. In the above regard, the Act defines "renewal application" to mean "*an application by an agency for a warrant in respect of a telecommunications service or person, being an application made while a warrant issued to the agency in respect of that service or person is still in force*". Proposed Section 119(3) states that "*an issuing authority must not vary a stored communications warrant by extending the period for which it is to be in force*" and Section 119(5) states that if a "*further warrant relates to the same telecommunications service as the previous warrant, it must not be issued within 3 days after the day on which the previous warrant was executed*" and the Explanatory Memorandum states that "time limit is to ensure that agencies are not able to get a new stored communications warrant daily, which would undermine the separate interception warrant regime". Hence it seems that "renewal applications" are not permitted in relation to stored communications warrants.

90. We submit that either Section 162(2)(c) should be amended to refer to applications for "further warrants" in respect of the same telecommunications service or person, or that the definition of "renewal application" needs to be amended to specify its meaning in relation to stored communication warrants (e.g. applications for "further warrants") in addition to its existing meaning in relation to interception warrants.

Recommendation:

That the Bill be amended to delete, or specify the meaning of, the references to "renewal applications" in relation to stored communications warrants.

3.3.4(c) Minister's powers to seek information from agencies

91. The heading of Section 160 is "Minister may seek further information from Commonwealth agency" but the remainder of the section refers apparently to any enforcement agency, not only Commonwealth agencies.

92. In the context of other provisions relating to stored communications, we assume that the heading is wrong, not the text of the section. Accordingly, we submit that for the purposes of certainty the heading should be amended to refer to "enforcement agencies" instead of "Commonwealth agency".

Recommendation:

That the heading or content, as applicable, of Section 160 be amended to eliminate doubt/questions as to the Minister's powers.

▲ Go to Contents List

3.3.5 Additional Safeguards Necessary

93. As stated above, EFA considers that the reduced record keeping and inspection provisions combined with the proposed reduced reporting requirements result in inadequate safeguards and controls against misuse. The covert nature of searches at telecommunications service providers' premises together with the high potential for invasion of privacy of non−suspect individuals necessitates stronger safeguards and controls than are contained in the Bill.

3.3.5(a) Notification to Individuals

94. In relation to interception warrants, the 1994 Barrett Report recommended that:

> *'agencies should be required to notify any innocent person whose telephone service has been intercepted of the fact of interception within a period of 90 days of the cessation of the interception. If this proposal is not accepted, agencies should be required to maintain a*

register of incidents where the telephone service of an innocent person has been intercepted; the register should be made available to the relevant inspecting agency for inspection and report to the Attorney General'.

and stated that:

'the objectives of the [notification] requirement would be two−fold − to enhance the privacy protection for innocent persons and to impose an added discipline on law enforcement agencies to exercise great care in deciding whether to apply for warrants.'[11]

95. While the then government did not accept the notification recommendation, the TI Act was amended in 1995[12] with provisions establishing "a new special register with details of warrants which do not lead, directly or indirectly, to a prosecution" which the government considered would "provide a similar level of protection against misuse".

96. The special register provisions still exist as a protection against misuse of interception powers, however the Bill contains no similar protection against misuse of, in effect, covert search powers at telecommunications service providers' premises.

97. We also note that the Senate Scrutiny of Bills Committee Report on the Inquiry into Entry and Search Provisions in Commonwealth Legislation[13] states that the AFP, in seeking power to conduct covert searches at premises, suggested safeguards which included a requirement of "notifying the occupier of the details of any covert search once charges were preferred, or an investigation finalised, or the reasons for the investigation remaining covert no longer applied".

98. EFA considers that individuals who have been the subject of covert surveillance by way of accessing their communications at a telecommunications service provider's premises should be notified of the details of that covert search/surveillance within 90 days of the date of access.

3.3.4(b) Public Interest Monitor

99. If it is not required that individuals be notified, a Public Interest Monitor should be involved in the granting of warrants.

100. Such a role should include functions similar to the Queensland Public Interest Monitor which include, among other things, to appear at any hearing of an application for a surveillance warrant or covert search warrant to test the validity of the application, and for that purpose at the hearing:

"*(i) present questions for the applicant to answer and examine or cross−examine any witness; and*
(ii) make submissions on the appropriateness of granting the application;
and
(c) to gather statistical information about the use and effectiveness of surveillance warrants and covert search warrants; and
(d) whenever the public interest monitor considers it appropriate−−to give to the commissioner a report on noncompliance by police officers with this part."
(*Queensland Police Powers and Responsibilities Act 1997*, Section 159[14])

101. In addition, Public Interest Monitors' functions should include a role in relation to monitoring execution of warrants including the extent of collection of irrelevant communications of the suspect and of non−suspects and whether such privacy intrusions significantly outweigh the collection of communications relating to criminal conduct.

Recommendation:

That the Bill be amended to require notification to individuals in accord with the Barrett Report recommendation; or require that a Public Interest Monitor be involved in the granting of warrants.

▲ Go to Contents List

3.4 Compulsory Notices to Produce served on carriers

102. The Explanatory Memorandum states:

> "*The reference to the knowledge of the intended recipient is designed to protect the privacy of the communication before such time as the communication becomes accessible to the intended recipient. 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. For example,* ***an enforcement agency may use its existing notice to produce at the carrier where they have notified the intended recipient that they intend to access the communications in this manner.***
>
> *This distinction means that enforcement agencies are regulated by the stored communications regime only when they are acting covertly in the access to these communications. When acting overtly, existing access and compulsion powers of the enforcement agencies remain applicable."* (emphasis added)

103. EFA is opposed to agencies being 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. This results in two serious issues:

- there is potential for misuse of these powers, i.e. failure to notify, by Commonwealth, State and Territory criminal law, civil penalty and public revenue enforcement agencies.
- carriers [includes ISPs] who disclose the content of communications could, it appears, be sued by a customer who had not been notified, under the civil remedy provisions of the *Telecommunications Act 1997*.

104. In addition, we are concerned by the situation in relation to compulsory notices to produce issued by e.g. ASIC. For example, as stated in the Committee's July 2004 Report on the TIA(SC) Bill[15]:

> "*3.33 The representative of ASIC went on to note that in its view, if the Bill was enacted, ASIC would be able to use compulsory notices to access all emails stored at an ISP, whether they had been read or not:*
>
> > *'At least some of our compulsory notice powers are quite restricted in terms of what we could require production of, but they do not actually require that an offence has been committed or that we have suspicion that an offence has been committed before we can serve them. ...'"*

105. Agencies most certainly should not be permitted to serve their own compulsory notices to produce on telecommunications service providers when there is no suspicion that an offence has been committed as referred to by ASIC above.

106. Furthermore, the remarks by ASIC above, and in the Explanatory Memorandum, show that there is a serious lack of clarity in telecommunications legislation concerning whether or not ASIC has in fact been

authorised to obtain content of stored communications in the above manner, and in relation to the situation after enactment of the current Bill.

107. Section 280 of the *Telecommunications Act 1997*[16] states:

> "*280 Authorisation by or under law*
> *(1) Division 2 does not prohibit a disclosure [by a carrier] or use of information or a document if:*
> *(a) 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; or*
> *(b) in any other case−the disclosure or use is required or authorised by or under law.*
> *(2) In this section:*
> *enforcement agency has the same meaning as in section 282.*"

108. The current Bill also defines enforcement agency by reference to Section 282 of that Act.

109. Section 282(10)[17] states:

> "enforcement agency means:
> (a) a criminal law−enforcement agency; or
> (b) a civil penalty−enforcement agency; or
> (c) a public revenue agency."

110. In our view, the above sections make clear that information cannot be disclosed by carriers under Section 280 to enforcement agencies unless they have a warrant (and our understanding is that following enactment of the current Bill, it will over−ride Section 280 in relation to stored communications and therefore a stored communications warrant will be necessary). A carrier would appear justified in declining to provide content of communications in response to a "compulsory notice" on the ground that ASIC is a civil enforcement agency (which is defined to mean "an agency responsible for administering a law imposing a pecuniary penalty") and therefore is required to obtain a warrant. If ASIC or any other Commonwealth, State or Territory enforcement agency with similar powers has a different interpretation of the *Telecommunications Act 1997* then an argument between the agency and the carrier appears likely to ensue given carriers risk criminal and/or civil action if they disclose information in breach of either the *Telecommunications Act 1997* or the *Telecommunications (Interception) Act 1979*.

Recommendation:

That the Bill be amended to include provisions amending Section 280 of the *Telecommunications (Interception) Act 1979*, effective from the same date as the Bill, to make clear than an enforcement agency as defined in Section 282 of that Act must provide a stored communications warrant in order to access stored communications.

▲ Go to Contents List

3.5 Legal professional and parliamentary privilege

111. Searches of the covert nature that occurs under warrant (or notice to produce without prior notification to the relevant individual) at telecommunications service providers' premises unduly infringe legal professional privilege (and also other common law privilege, e.g. Parliamentary privilege).

112. While over−riding legal professional privilege in intercepting "live" telephone calls has been regarded as justifiable because it is largely unavoidable[18], in our view it is not justifiable in relation to accessing stored

communications by way of executing a warrant at a third party telecommunications service provider's premises.

113. In the case of search warrants executed on an individual's own premises, the individual is generally given the opportunity to be present and have a lawyer present and is entitled to raise legal professional privilege in relation to relevant documents[19]. No such opportunity is available in the case of searches at a telecommunications service providers' premises and the 'occupier' of those premises is certainly not in a position to know whether the stored communications include communications that are the subject of legal professional privilege.

114. We observe that, in relation to the ACCC's compulsory notice issuing powers, the *Trade Practices Legislation Amendment Bill (No. 1) 2005*[20] inserts a new subsection 155(7B) which states that:

> "*This section does not require a person to produce a document that would disclose information that is the subject of legal professional privilege.*"

and the Explanatory Memorandum states that:

> "*The insertion of subsection 155(7B) implements recommendation 13.5 of the Dawson Review which stated that section 155 should be amended to ensure that the TP Act does not require the production of documents to which legal professional privilege attaches. The Government endorsed this recommendation because preserving legal professional privilege is in the public interest, as it facilitates the obtaining of legal advice and promotes the observance of the law.*"

115. We agree that preserving legal professional privilege is important for the above reasons and consider that efforts should be made to preserve same, to the greatest extent possible, in relation to accessing communications from third parties who are telecommunications service providers. We do not consider the general rules in relation to admissible evidence are adequate in that regard. Privileged communications should not be permitted to be seized in the foregoing circumstances in the first place, other than in instances of genuine urgency in connection with serious criminal offences.

116. While agencies such as ASIC, ACCC, ATO, etc are empowered to serve notices to produce on third parties such as banks and financial institutions, such organisations are unlikely to be in possession of their clients' communications that are privileged between a client and his/her lawyer. However communications between an individual and his/her lawyer are likely to be among communications stored on a telecommunications service provider's equipment, especially given that agencies are and will be permitted to access communications that have not been collected by the intended recipient and therefore an individual does not have an opportunity to delete privileged communications from the service provider's system/equipment.

117. Although the ACCC's proposed powers referred to above would not *require* a telecommunications service provider to disclose a customer's or other person's information that is the subject of legal professional privilege, a service provider is not in a position to know whether communications of customers and other persons stored on their equipment includes such communications, therefore they should not be served with such notices.

118. Civil penalty enforcement and public revenue agencies should not be permitted to obtain stored communications from telecommunications service providers unless they have obtained the same warrant (by providing the same information and satisfying the same issuing requirements and conditions) as criminal law enforcement agencies would be required to obtain in the same circumstances.

119. The preservation of legal professional privilege should be a matter required to taken into consideration in the issue and execution of warrants executed at telecommunications service provider's premises. If the

stored communications are likely to include communications the subject of legal professional privilege, the communications sought to be seized should be required to be placed in the confidential safekeeping of an independent person and the relevant individual provided with the opportunity to prevent disclosure of any such communications to the agency, by way of liaison with the agency and if that fails by application to the issuer of the warrant.

▲ Go to Contents List

4. Interception of Communications

4.1 Innocent Party Interceptions

120. EFA strongly objects to the so−called "B−Party" provisions which vastly expand the circumstances in which, and the frequency with which, non−suspects' telecommunications services may be intercepted and monitored. No adequate justification for this proposal has been provided and, even if it had been, the circumstances in which interception and surveillance of innocent persons' communications would be permitted is not sufficiently limited, nor would adequate controls and safeguards be in place.

121. While the Second Reading[21] speech states that:

> "*The issuing authority must also have regard to the following additional factors:*
> *− how much the privacy of any person would be likely to be interfered with by the interception, the gravity or seriousness of the offences being investigated,*
> *− how much the intercepted information would be likely to assist with the investigation by the agency of the offence,*
> *− to what extent alternative methods of investigating the offence have been used by, or are available to, the agency,*
> *− how much the use of such methods would be likely to assist in the investigation by the agency of the offence, and*
> *− how much the use of such methods would be likely to prejudice the investigation by the agency of the offence.*"

122. the above factors are no different from the long existing factors that apply to the issue of an interception warrant in respect of a person who **is suspected** of being involved in an offence.

123. The only new provisions proposed to create the "limited and controlled circumstances" claimed in the Explanatory Memorandum are:

> "*(3) The Judge or nominated AAT member must not issue a warrant in a case in which subparagraph (1)(d)(ii) applies unless he or she is satisfied that:*
> *(a) the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person involved in the offence or offences referred to in paragraph (1)(d); or*
> *(b) interception of communications made to or from a telecommunications service used or likely to be used by that person would not otherwise be possible.*"

124. The above provisions are wholly inadequate. It seems clear that a law enforcement agency could simply inform an issuing authority that the suspect always uses a public telephone in order to obtain warrant/s authorising interception of one or more innocent persons' telecommunications services. An issuing authority would have no means of knowing whether or not it is a fact that the suspect only uses public telephones.

125. Among many other things, it is of massive concern that these provisions could be used to intercept the telephone services of non−suspect persons who are, for example, lawyers or other persons who make and receive many calls that are subject to legal professional, or other, privilege.

126. Furthermore, the Bill does not implement the controls suggested in the Blunn Report in relation to innocent party interceptions which were:

- "*a requirement that any agency requesting such a 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 [to the satisfaction of the issuing authority] that* ***[the information material to the investigation] cannot be obtained other than by*** *telecommunications interception or the use of a listening device*"
- "***destruction of non−material content in whatever form should be strictly supervised***"
- "*the number and justification of B−Party intercept warrants should be* ***separately*** *recorded by the Agency Co−ordinator and reported to the Attorney−General*"
- "*the use of such warrants should be* ***separately*** *reported to the Parliament*"
(emphasis added)

127. The Bill does not contain any of the above controls.

128. Moreover, although the Explanatory Memorandum states:

> "*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. Generally, lawfully obtained information must be destroyed unless a purpose in connection with the investigation of an offence punishable by a maximum period of imprisonment of at least three years.*"

129. the existing destruction provisions have been insufficiently effective since 2000 and are of themselves a matter for law reform as recommended in the Sherman Report (irrespective of whether new B−Party warrant provisions were to be implemented). 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. Furthermore, as pointed out in the Ford Report[22], up to 90 electronic copies of intercepted information may be retained by agencies in addition to copies in the form of printed transcripts, etc. (For further information and ease of reference, see relevant extracts from the Sherman and Ford Reports provided in Appendix 1.)

130. EFA is not persuaded that there is sufficient, if any, justification to expand the circumstances in which an innocent/non−suspect's communications may be intercepted. Accordingly we consider the so−called "B−Party" provisions should be deleted from the Bill.

131. If, at some future time, we were to become persuaded that such interceptions should be permitted in some clearly specified and limited circumstances, we would consider that, at the very least, the following safeguards and controls would need to be implemented:

f. **Higher evidentiary threshold for granting a warrant**
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.

There should also be an onus on agencies to provide evidence as to the nature of the telecommunications service that is to be intercepted, e.g. Private or business line? What kind of business? High or low volume of calls? etc. in order to provide the issuing authority with relevant information to be considered in relation to the potential extent of invasion of privacy of innocent

party communications (that is, not only the innocent B−Party, but other innocent persons with whom the B−Party communicates).

a. **Greater scrutiny/testing of the evidence**
A Public Interest Monitor should be required to be involved in the granting of warrants, to assist the issuing authority to consider the privacy implications etc, and as outlined in Section 3.3.5(b) earlier herein.

b. **Prohibition on issue of warrants where the B−Party is a lawyer, etc.**
Under no circumstances should B−Party warrants be allowed to be issued for interception of telecommunications services of persons who are, for example, lawyers or other persons who make and receive many calls that are subject to legal professional, or other, privilege.

c. **Reduced duration of warrant**
Warrants should be limited to 14 days duration (not 30−45 days as in the Bill) and should not be renewable unless during that 14 days information material to the investigation had been obtained from such interception and further such information was likely to be obtained from continued interception and would still not be able to be obtained by any means other than interception of the same (B−Party) telecommunications service. The duration of a renewed warrant should not be permitted to be more than 30 days.

e. **Copying and Destruction of 'non−material content'**
No copies of recordings should be permitted to be made prior to review of the original recording to ascertain whether or not it involves the suspect. The agency should be required to destroy any interception product, in whatever form, that does not involve the suspect immediately on it becoming apparent that it does not involve the suspect.

In addition, and whether or not B−Party interceptions are permitted, the destruction provisions of the Act should be updated in relation to all intercepted information and records in a manner substantially the same as those contained in the *Surveillance Devices Act 2005*, including to require that information be "kept in a secure place that is not accessible to people who are not entitled to deal with the record or report" and to require review/destruction of information at least every 5 years after an initial decision to retain it.

d. **Enhanced Reporting**
All of the existing reporting provisions (numbers, justification, use, etc) applicable to interception warrants should apply to so−called B−Party interception warrants, but all of the B−Party related information should be reported on in separate sections of the reports to the (C'th) Minister and to the Parliament.

Recommendation:

That "Schedule 2 − B−Party Interception" be deleted from the Bill.

▲ Go to Contents List

4.2 Equipment−based interception / Telecommunications Device Warrants

132. EFA has serious concerns about the amendments to the named person interception warrant provisions to enable interception agencies to intercept communications to and from telecommunications equipment ("device") identified by a "telecommunications number". 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.

133. The provisions enable an agency to apply for a warrant when:

> *"(c) there are reasonable grounds for suspecting that a particular person is using, or is likely to use, more than one telecommunications service; and*
> *(d) information that would be likely to be obtained by intercepting under a warrant:*
> *(i) communications made to or from any telecommunications service that* ***the person*** *is using, or is likely to use; or*
> *(ii) communications made by means of a particular telecommunications device that* ***a person*** *is using, or is likely to use;*
> *would be likely to assist in connection with the investigation by the agency of a serious offence, or serious offences, in which* ***the person*** *is involved; and* " (emphasis added)

134. We note new clause (d)(ii) above refers to "a person", not to "the particular person" or "the person". Hence, it seems clear that these provisions are intended to permit interception of communications made to or from a B−Party's equipment. This also seems apparent from the Second Reading speech[23] which discusses the B−Party Schedule and immediately thereafter states that the equipment−based provisions are "likewise".

135. While the Blunn Report briefly discussed equipment−based interception proposals, Mr Blunn did **not** recommend that such warrants be implemented. According to the Second Reading speech: "*Equipment based interception will enable the interception of communications through a single piece of hardware, such as a mobile telephone handset*". However, as was pointed out in the Blunn Report, there is no device number that uniquely identifies mobile phone handsets:

> "*3.2.3. A potentially more promising system of identifying the user [than the International Mobile Service Identifier (IMSI) which attaches to a Subscriber Identity Module (SIM)] would appear to be attempts to utilise the International Mobile Equipment Identifier (IMEI) which is intended to be a unique electronic serial number allocated to each GSM handset. However in practice multiple IMEIs exist i.e. multiple handsets have the same IMEI. Unlike the SIM problem which now seems insoluble the situation with IMEIs does hold some hope of resolution but it would require determined action by regulators and carriers with significant public impact. For any system based on IMEIs to be used effectively would also require a different legal approach to the basis for access as it appears that such a system would not meet the requirements of the Interception Act that a warrant must only be issued in relation to a 'service'. If the IMEI system is to be developed it would therefore seem necessary to review the concept of service.* ***Whatever the solution it would be imperative that some system be devised which provides for the effective identification of the means of communication.***
>
> *3.2.4. Under the named person warrant regime, a warrant may be issued in respect of a person who is alleged to have committed or is likely to commit a prescribed offence or engaged in, or likely to engage in, activities prejudicial to security and who it is believed is using or is likely to use more than one telecommunications service. The warrant is an effective tool to assist with the investigation of targets that use multiple SIMs. In this instance it may be possible to make use of interception based on IMEI as a tool to facilitate interception. I understand that the comprehensive reporting arrangements in the Interception Act currently prohibit interception based on IMEI; however I am of the view that there is a basis to consider the possibility.*
>
> *3.2.5.* ***Accordingly, I recommend that priority be given to developing a unique and indelible identifier of the source of telecommunications and therefore as a basis for access.***" (emphasis added)

136. (See also, regarding non−uniqueness of IMEI numbers, BBC UK news report *Phone firms defend security record*[24] and Vodaphone Australia web site page[25].)

137. EFA considers it highly inappropriate to permit equipment−based interception prior to the development of a "unique and indelible identifier of the source of telecommunications" as a basis for access.

138. EFA is strongly opposed to warrants being issued based on "device numbers" that may identify multiple items of equipment, due to the potential for interception of communications sent to or from a device that is not used by the suspect but has the same number as another device that is used by the suspect.

139. Although the Explanatory Memorandum states:

> "*The requirement that a telecommunications number or identifying factor be unique is designed to ensure that interception only occur where an interception agency is able to identify the particular telecommunications device that is to be the subject of telecommunications interception.*"

140. there is no requirement that the "telecommunications number" (or "other identifying factor") of the "telecommunications device" be advised to the issuing authority, nor any requirement that the issuing authority be satisfied that the device can, in fact, be uniquely identified by a number.

141. Moreover, there is no requirement that the interception agency know the so−called unique identifying number prior to applying for a warrant. Apparently it is intended that interception agencies will expect carriers to work out which telecommunications device is being referred to by "a description in writing of the device sufficient to identify it" provided by the agency (see, for example, proposed Section 60(4A)). Such description apparently does not have to be provided to the issuing authority. Hence, it appears that a carrier who considered the description to be inadequate to **uniquely identify** a device and hence declined to take action to enable the interception warrant to be executed may risk facing proceedings for obstructing or hindering a person acting under a warrant (s106). While a person may do so if they have a "reasonable excuse", the defendant bears an evidential burden in relation to the matter. This situation constitutes a risk that carriers will facilitate interceptions in the absence of adequate surety that a number does uniquely identify the subject device and no other device.

142. EFA considers that if a device is uniquely identifiable by a number, then that number should have to be specified in the warrant. However, we are doubtful that any current telecommunications devices are uniquely identifiable by a number that can be used for the purpose of identifying and capturing real−time communications being made to and from a particular device and only that device. We question whether that is why the vast majority of types of numbers listed in the Bill identify a telecommunications **service** − none of them uniquely and indelibly identify a telecommunications device:

> "*telecommunications number means the address used by a carrier for the purposes of directing a communication to its intended destination and identifying the origin of the communication, and includes:*
> *(a) a telephone number; and*
> *(b) a mobile telephone number; and*
> *(c) a unique identifier for a telecommunications device (for example, an electronic serial number* [presumably an IMEI number] *or a Media Access Control address); and*
> *(d) a user account identifier; and*
> *(e) an Internet Protocol address; and*
> *(f) an email address.*"

143. All of the above "numbers" other than (c) identify telecommunications services which are already able to be intercepted with a named person, or telecommunications service, warrant. Hence the intent and objective of claiming these identify a "device" is entirely unclear.

144. For example, how is "(a) a telephone number" to be used in this regard? Is it intended that an interception agency provide a landline telephone number (claimed to be "a description in writing of the

device sufficient to identify it") to an ISP and expect the ISP to search its records for a customer with an ADSL Internet access service connected via that landline telephone number and then facilitate interception of all communications being made to or from the customer's ADSL modem? If not, what is the intent? (To date, EFA has been unable to conceive of any usages of the "numbers" above that would not be similar to the foregoing.) If that is the intent, then the purpose is highly questionable because interception agencies can already obtain warrants to intercept communications travelling over a telephone line (to and from a telephone number) and/or obtain a warrant to intercept communications travelling to and from the Internet Protocol address assigned by the ISP to a customer's Internet access account/ADSL modem.

145. Accordingly, it appears that a primary purpose of telecommunications device warrants may be to enable interception of B−Party communications, that is, communications to and from a device belonging to a person who is not a suspect given that, as mentioned above, agencies would be able to apply for warrants in relation to "communications made by means of a particular telecommunications device that **a person** is using, or is likely to use" not necessarily the person named in the warrant. For example, if an agency knows that a suspect uses another person's landline telephone and knows that telephone number, it appears they could obtain a warrant to intercept communications to and from that other person's (non−suspect's) ADSL modem.

146. If the above is not the purpose, then a major overhaul of the definitions and provisions in "Schedule 3−Equipment−based interception" needs to be undertaken to make clear what is intended. Any such amendments should be made the subject of a separate Parliamentary inquiry.

147. In addition to our concerns about lack of clarity as to intent and purpose set out above, we question the merits and benefit of attempting to use a Media Access Control address as referred to in (c) above. We recommend the proponents of this idea read the paper *Using MAC Addresses in the Lawful Interception of IP Traffic*[25] by Branch, Pavlicic and Armitage of the Centre for Advanced Internet Architectures at Swinburne University, which was presented to the Australian Telecommunications Networks & Applications Conference December 2004:

> "*In this paper we report on our investigations into the feasibility of using MAC addresses rather than IP addresses as an identifier in Lawful Interception. We found that MAC address interception in PPPoE and Broadband Ethernet environments can be very easily subverted. Consequently, we believe that MAC based interception is a poor option for lawful interception.*
> ...
> *One of the possible identifiers proposed in the recently released ETSI Technical Standard describing service specific interception is to attempt to intercept traffic based on the end user's MAC address. In this case interception devices would be configured to capture traffic to or from user devices with a specific MAC address. This does not address the Internet kiosk scenario, but it does provide some mechanism of interception where the targeted user consistently uses the same device (such as a laptop computer or PDA) to access their communications. Of course linking MAC address to individual users is an issue in itself that is beyond the scope of this paper. In this paper we assume that a targeted individual's MAC address is known and we investigate how effective interception based on MAC address is.*
> ...
> *We then investigated the effects of spoofing the MAC address in the PPPoE system. The MAC address, although a hardware address burnt into the Ethernet card when it is manufactured, can be spoofed. We used readily available software that modified the MAC address placed in the Ethernet frames.*
> ...
> *Our work shows that MAC address interception is almost trivial to subvert. We believe interception based on MAC address will completely ineffective, even if the issue of linking identity to MAC address is solved. Consequently, we think that the ETSI standard should remove it from the list of possible target identifiers, or at least note the ease with which interception based on it can be subverted.*

...
We will continue our work in this area by investigating other mechanisms that incorporate procedural as well as technical approaches."

148. Interception agencies are already able to obtain an interception warrant to intercept communications by way of the more reliable and effective method of an Internet Protocol address assigned by an ISP's system to a user. Equipment−based warrants to enable use of a MAC address (which can be changed by the user as pointed out above) are not necessary.

Recommendation:

That "Schedule 3−Equipment−based interception" be deleted from the Bill.

▲ Go to Contents List

5. Conclusion

149. EFA generally supports the stored communications access regime proposed to be implemented by the Bill. In our view, it is apparent that the Government has made a genuine effort to appropriately resolve the complex issues that have arisen during the course of inquiries into prior Bills, with the intention of giving significantly more effect to the *Telecommunications (Interception) Act*'s primary objective of protecting the privacy of individuals who use the Australian telecommunications system, including those who use new telecommunications technologies such as email, SMS and voice mail to communicate.

150. The stored communications provisions of the Bill will unquestionably result in a vastly more appropriate situation than has existed since December 2004 and for that reason EFA generally supports passage of the provisions. However, we consider it important that the definitional issues raised herein be addressed prior to passage, and we would greatly prefer that other improvements suggested in this submission be made. Recognising the approaching sunset clause deadline of 15 June, we realise that as a practical matter, it would be unlikely to be possible to arrange some improvements suggested (e.g. Public Interest Monitor) prior to that date. We consider that implementation of improvements that could not be achieved prior to 15 June should be considered in conjunction with the Government's ongoing review of telecommunications legislation following the Blunn Review.

151. EFA supports the deletion of the outdated exception to the prohibition on interception, often referred to as the "participant monitoring" exception, which we understand some businesses and other organisations perceive as permitting them to covertly monitor and record incoming calls.

152. EFA is strongly opposed to the so−called "B−Party" interception provisions of the Bill which vastly expand the circumstances in which, and the frequency with which, non−suspects' telecommunications services may be intercepted and monitored. "Schedule 2 − B−Party Interception" must be deleted from the Bill.

153. EFA is also strongly opposed to the "equipment−based" interception provisions. In our view the provisions are technically incomprehensible. To the extent that they may be comprehensible, it appears the primary purpose is probably to enable interception of communications to and from B−Party equipment such as modems and computers. If that is not the purpose, then a major overhaul of the definitions and provisions in Schedule 3 needs to be undertaken to make clear what is intended. Any such amendments should be made the subject of a separate Parliamentary inquiry at some future time. "Schedule 3 − Equipment−based interception" must be deleted from the Bill.

▲ Go to Contents List

References

1. Senate Legal &Constitutional Legislation Committee, Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2006
<http://www.aph.gov.au/senate/committee/legcon_ctte/ti/index.htm>

2. EFA submission to the Review of the Regulation of Access to Communications under the Telecommunications (Interception) Act 1979, 20 May 2005
<http://www.efa.org.au/Publish/efasubm−agd−tiactreview2005.html>

3. *Telecommunications (Interception) Amendment Bill 2006*
<http://parlinfoweb.aph.gov.au/piweb/browse.aspx?path=Legislation%20%3E%20Current%20Bills%20by%20Portfolio%20%3E%20Attorney−General%20portfolio%20%3E%20Telecommunications%20(Interception)%20Amendment%20Bill%202006>

4. Blunn Report on the Review of the Regulation of Access to Communications, August 2005
<http://www.ag.gov.au/agd/WWW/agdHome.nsf/Page/Publications_2005_Report_of_the_Review_of_the_Regulation_of_Access_to_Communications_−_August_2005>

5. *Telecommunications (Interception) Act 1979*
<http://www.austlii.edu.au/au/legis/cth/consol_act/ta1979350/>

6. Explanatory Memorandum, *Telecommunications (Interception) Amendment Bill 2006*
<http://parlinfoweb.aph.gov.au/piweb/browse.aspx?path=Legislation%20%3E%20Current%20Bills%20by%20Portfolio%20%3E%20Attorney−General%20portfolio%20%3E%20Telecommunications%20(Interception)%20Amendment%20Bill%202006>

7. *Crimes Act 1914* (Cth) subsection 3LB
<http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3lb.html>

8. *Crimes Act 1914* (Cth) subsection 3L(1)
<http://www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3l.html>

9. Report of Review of Named Person Warrants and Other Matters Telecommunications (Interception) Act 1979, Tom Sherman AO, June 2003
<http://www.ag.gov.au/agd/WWW/agdHome.nsf/Page/Publications_Publications_2003_Report_of_Review_of_Named_Person_Warrants_and_Other_Matters>

10. Telstra Submission to the Inquiry into the provisions of the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004, 29 June 2004
<http://www.aph.gov.au/senate/committee/legcon_ctte/completed_inquiries/2002−04/TI_stored_data/submissions/sub10.pdf>

11. Barrett Report on the Review of the Long Term Cost Effectiveness of Telecommunications Interception, quoted in *Report By The [N.Z.] Privacy Commissioner To The Minister Of Justice On Parts V And Viii Of The Harassment And Criminal Associations Bill (Interception Of Private Communications)*
<http://www.privacy.org.nz/people/intercpt.html>

12. Telecommunications (Interception) Amendment Bill 1994 [1995]: Second Reading, House Hansard, 01 December, 1995
<http://parlinfoweb.aph.gov.au/piweb/translatewipilink.ASPX?Folder=HANSARDR&Criteria=DOC_DATE:1995−12−01;SEQ_NUM:8>

13. Senate Standing Committee for the Scrutiny of Bills, Report on the Inquiry into Entry and Search Provisions in Commonwealth Legislation, 6 April 2000
<http://www.aph.gov.au/senate/committee/scrutiny/bills/2000/b04.pdf>

14. *Queensland Police Powers and Responsibilities Act 1997*, Section 159
<http://www.austlii.edu.au/au/legis/qld/consol_act/ppara2000365/s159.html>

15. Senate Legal & Constitutional Legislation Committee, Report on Inquiry into the Telecommunications (Interception) Amendment (Stored Communications) Bill 2004, July 2004
<http://www.aph.gov.au/senate/committee/legcon_ctte/TI_stored_data/report/report.pdf>

16. Section 280 of the *Telecommunications Act 1997*
<http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/s280.html>

17. Section 282 of the *Telecommunications Act 1997*
<http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/s282.html>

18. *Carmody v Mackellar [1997] 839 FCA; (1997) 76 FCR 115*, 30 July 1997
<http://www.austlii.edu.au/cgi−bin/disp.pl/au/cases/cth/federal_ct/1997/839.html>

19. Discussed in *Kennedy v Baker [2004] FCA 562; (2004) 135 FCR 520*, 6 May 2004
<http://www.austlii.edu.au/au/cases/cth/federal_ct/2004/562.html>

20. *Trade Practices Legislation Amendment Bill (No. 1) 2005*
<http://parlinfoweb.aph.gov.au/piweb/browse.aspx?path=Legislation %20%3E%20Current%20 Bills%20by%20Title%20%3E%20Trade%20Practices%20Legislation%20Amendment%20Bill %20(No.%201)%202005>

21. Second Reading speech, *Telecommunications (Interception) Amendment Bill 2006*, House Hansard.
<http://parlinfoweb.aph.gov.au/piweb/view_document.aspx?ID=2533569t;

22. Telecommunications Interception Policy Review, Peter Ford, First Assistant Secretary, Information and Security Law Division, Attorney−General's Department, May 1999
<http://www.law.gov.au/agd/Department/Publications/publications/ teleintreview/teleintreview.html>

23. See note 21.

24. Phone firms defend security record, BBC UK, 8 Jan 2002
"*New IMEIs can be programmed into stolen handsets and 10% of IMEIs are not unique.*"
<http://news.bbc.co.uk/2/hi/uk_news/1749215.stm>

25. Vodaphone Australia web site
"*It may be that some handsets share the same IMEI numbers. If a customer requests a block which Vodafone subsequently discovers affects another customer's usage of Vodafone's mobile service, Vodafone may not action the initial blocking request.*"
<http://www.vodafone.com.au/foryou/mobiles/handsetBlock.jsp>

26. *Using MAC Addresses in the Lawful Interception of IP Traffic*, P. Branch, A. Pavlicic and G. Armitage, Centre for Advanced Internet Architectures, Swinburne University. Presented to the Australian Telecommunications Networks & Applications Conference, December 2004
<http://caia.swin.edu.au/pubs/ATNAC04/branch−pavlicic−armitage−ATNAC2004.pdf>

▲ Go to Contents List

About EFA

Electronic Frontiers Australia Inc. ("EFA") is a non−profit national organisation representing Internet users concerned with on−line rights and freedoms. EFA was established in January 1994 and incorporated under the *Associations Incorporation Act* (S.A.) in May 1994.

EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting online civil liberties. EFA members and supporters come from all parts of Australia and from diverse backgrounds.

Our major objectives are to protect and promote the civil liberties of users of computer based communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of computer based communications systems.

EFA policy formulation, decision making and oversight of organisational activities are the responsibility of the EFA Board of Management. The ten elected Board Members act in a voluntary capacity; they are not remunerated for time spent on EFA activities. The role of Executive Director was established in 1999 and reports to the Board.

EFA has long been an advocate for the privacy rights of users of the Internet and other telecommunications and computer based communication systems. EFA's Executive Director was an invited member of the Federal Privacy Commissioner's National Privacy Principles Guidelines Reference Group and the Research Reference Committee (2001) and the Privacy Consultative Group (2004−2005). EFA participated in NOIE's Privacy Impact Assessment Consultative Group relating to the development of a Commonwealth Government Authentication Framework (2003), Centrelink's Voice Authentication Initiative Privacy Impact Assessment Consultative Group (2004), the ENUM Privacy and Security Working Group convened by the Australian Communications Authority ("ACA") (2003−2005), and the ACA's Consumer Consultative Forum meeting (April 2005). EFA has presented written and oral testimony to Federal Parliamentary Committee and government agency inquiries into privacy related matters, including amendments to the Privacy Act 1988 to cover the private sector, telecommunications interception laws, cybercrime, spam, etc.

▲ Go to Contents List

Appendix 1 − No requirement to destroy copies of irrelevant intercepted information

Extract from Ford Report 1999:

> "*2.3.7 [D]uring a record of interview, an officer might play (say) 30 intercepted calls to a suspect who had been the subject of an interception warrant, the suspect being a party to the calls. A single video and two audio copies of the interview might be made. Later a transcript of the interview is made and saved on a file server. The server is backed−up on a series of magnetic tapes. There are up to 90 back−up copies made of all documents. A number of copies of the transcript might be printed, some in draft form others in a final form.*
>
> 2.3.8 *In another example during a hearing, a series of (say) 60 intercepted calls might be played to suspect persons who were parties to the calls. Two audio copies are made of the hearing by the court reporter and notes and summaries of the calls are made by counsel. A transcript of the hearing is prepared and again stored on a file server back−up and several copies printed.*"

Extract from Sherman Report 2003:

> "*258. The Telecommunications (Interception) Legislation Amendment Act 2000 which introduced named person warrants also modified the definition of restricted record to simplify agency record keeping requirements. A restricted record is now defined in section 5 of the Interception Act as*
> *'a record, other than a copy, that was obtained by means of an interception , whether or not in contravention of section 7(1), of a communication passing over a telecommunication system.'*
>
> *259. The phrase 'other than a copy' was added by the 2000 amendments and this had the effect of removing copies of restricted records from the record keeping and destruction requirements of the Interception Act.*
>
> *260. Those requirements are:*
> *− keeping restricted records in a secure place −section 35 (1) (f);*
> *− destroying restricted records when they are no longer required for a permitted purpose − section 79 (1); and*
> *− recording details of the custody and movement of the restricted record – section 81(1)(e).*
>
> *261. A number of the law enforcement interception agencies urged that this amendment be repealed because it has had a number of undesirable effects notably there is now no real control of copies of restricted records. But it should also be emphasized that this was not a uniform view. Some agencies were happy with the amendment which removed copies from the definition of restricted record.*
> *...*
> *263. The Federal Privacy Commissioner sums up the general concern in his submission.*
>
> > *'Other record keeping obligations relating to the use and giving of information in evidence apply to both original recordings and copies. The limited definition of "restricted record" has the effect of reducing the safeguards on the use, Report of review of named person warrants and other matters disclosure or handling of personal information collected in an intercepted recording.*
> > *The same safeguards that apply to the original recording should also apply to any copies, extracts or transcripts of the recording held by the relevant*

agencies. Otherwise there is little logic in the additional protections applying to the original recordings. Consideration should be given to amending the definition of "restricted recording" so that it is not limited to the original recording of an intercepted communication.'

...
264. The concern expressed by a number of law enforcement agencies is that under the wider definition of restricted record which previously existed there was much greater control exercised over copies by the specialist TI branches and it also ensured that all TI product was destroyed at an appropriate time. The main argument from agencies which were supportive of retaining the narrower definition was that it greatly reduced the administrative burden.

265. It has to be acknowledged that it is very difficult to control all information emanating from TI product. For example evidence of crucial conversations evidencing criminal conduct may be referred to in investigative reports or in briefs to the DPP. Copies of restricted records (whether relevant or not) have to be provided to defence teams.

266. However I believe there is a strong case that at least the copies of recordings and transcripts or other direct records of intercepted communications should be controlled in the same manner as original recordings. It is the material which has evidentiary value which needs to be controlled.
...
Recommendation No 8
The definition of restricted record which existed prior to the 2000 amendments to the Interception Act should be reinstated."

▲ Go to Contents List