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

9 March 2004

The Secretary
Senate Legal and Constitutional Committee
Room S1.61, Parliament House
Canberra ACT 2600

Email: legcon.sen@aph.gov.au

Dear Ms Gell

Inquiry into the provisions of the Telecommunications (Interception) Amendment Bill 2004

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

EFA appreciates the opportunity to make a submission and would be pleased to present oral testimony and respond to any questions Committee members may have. In the event that the Committee may wish to ask EFA to attend a hearing, with a view to assisting the Committee Secretariat in scheduling hearings, we advise that the most convenient venues for EFA are, in order of preference, Brisbane, Canberra, Sydney and Melbourne. We generally prefer, if convenient to the Committee, an early afternoon session so that if an EFA representative needs to travel from interstate, this can be done on the day of the hearing, in order to minimise travel costs, rather than requiring an overnight stay due to airline flight schedules (particularly during daylight saving months).

Yours sincerely

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)

Submission to the Senate Legal and Constitutional Legislation Committee

Inquiry into the provisions of the *Telecommunications (Interception) Amendment Bill 2004*

9 March 2004

Contents:

---

1. Executive Summary

- EFA supports the extension of the definition of "interception" to include reading or viewing a communication which thereby provides increased privacy protection for text based communications, such as email and SMS messages.

- EFA considers the proposed amendments in relation to communications stored while passing over a telecommunications system (e.g. email, SMS and voice mail messages) are a major improvement over the amendments that were proposed in 2002 in relation to the same matters. However, several aspects of the proposed amendments require clarification, and additional amendments are necessary. Unless additional amendments are made, the protection for stored communications provided by the amendments will be very weak and therefore inadequate to achieve the apparent intent of the Bill in that regard. In addition, absent additional amendments, the Bill appears likely to have probably unintended consequences in relation to admissibility of evidence and potential criminal or civil proceedings against some carrier employees.

- EFA opposes the extension of the availability of interception warrants to the proposed broad range of so−called "cybercrime" offences. Most of those listed in the Bill involve penalties of only 1, 3 or 5 years (instead of the 7 years normally applicable for interception warrant availability) and do not necessarily involve the use of a telecommunications system to commit the offence, notwithstanding that they are described as "cybercrime" offences in the Explanatory Memorandum.

- EFA opposes the proposed amendments in relation to ASIO because there does not appear to be any legitimate reason or need for the changes.

The above matters are addressed in detail in this submission.

Go to Contents List

2. Introduction − 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 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 Research Reference Committee during 2001. EFA participated in NOIE's privacy impact assessment consultative group relating to the development of a Commonwealth Government Authentication Framework in 2003 and is currently participating in the ENUM Privacy and Security Working Group convened by the Australian Communications Authority. EFA has presented oral testimony to Federal Parliamentary Committee inquiries into privacy related matters, including amendments to the Privacy Act 1988 to cover the private sector, telecommunications interception laws, cybercrime, etc.

Go to Contents List

3. Extended definition of "interception"

The existing *Telecommunications (Interception) Act 1979* ("the Act") defines "interception" as consisting of listening to or recording (which includes copying), by any means, a communication in its passage over a telecommunications system without the knowledge of the person making the communication.

The proposed amendments extend the definition of "interception" to include reading or viewing a communication during its passage over a telecommunications system.

EFA supports this change because the amended definition will provide increased privacy protection for text and visual messages, such as SMS, MMS and email, by making it illegal to view or read these messages during their passage over a telecommunications system. It also thereby ensures that law enforcement agencies have to obtain an interception warrant before intercepting and reading or viewing such messages.

▲ Go to Contents List

---

4. Delayed and stored communications

This section discusses the proposed amendments concerning communications temporarily delayed and stored during passage, for example, email, SMS, MMS and voice mail messages.

4.1 Background − Difference from 2002 Proposal

Some recent commentary in the media has stated that the proposed changes concerning stored communications are "similar" to changes proposed by the Federal Government in 2002, which EFA strongly opposed. While the proposed amendments deal with the same issue that the government sought to address in 2002, the Government has apparently re−visited that issue with the result that the 2004 proposal is the opposite of the 2002 proposal.

In 2002, the amendments proposed by the government deemed that messages temporarily stored during transit were **not** passing over a telecommunications system while they were temporarily stored. The effect of that change would have been to allow LEAs to access messages stored on telecommunications service providers' equipment, that had not been delivered to the intended recipient, without an interception warrant. It also would have introduced a risk of access to messages temporarily stored during passage without a warrant of any type due to existing provisions of Section 282 of the *Telecommunications Act 1997*. EFA opposed those changes because EFA considers that all telecommunications should be afforded the same level of protection during passage. The fact that the particular technology in use automatically results in temporary storage during passage should not be used as an excuse to afford email, SMS messages, etc, less privacy protection than ordinary telephone calls.

4.2 2004 Proposal

The 2004 proposal appears to ensure that messages temporarily stored during passage are afforded a similar level of privacy protection to ordinary telephone calls. An interception warrant is required until after a message has completed its passage which occurs, as set out in the proposed amendments, when the message:

- is read/accessed by the intended recipient (or a person authorised by the intended recipient), or
- is delivered to equipment the recipient can use to access the message without using a telecommunications system, for example, delivered to the recipient's computer, mobile phone handset, etc.

The proposed amendments appear to be in accord with EFA's submissions to the Committee's inquiry in 2002. EFA supports the amendments concerning stored messages, provided our interpretation of same is correct (as detailed below), because they provide a reasonable degree of protection to Internet users that is not dissimilar to that currently accorded to telephone users. The existing law is insufficiently clear in this area and the clarification provided by these amendments is certainly needed.

The proposed amendments introduce the concept of 'delayed access message services'. These services include fixed line and mobile voicemail, SMS, MMS, email and any other are service where there is a delay between the sending of the communication and its ultimate receipt by the intended recipient. During the delay the communication is or may be temporarily stored on a service provider's equipment. For example, email is stored on an ISP's equipment pending download to the intended recipient's computer and voice mail messages are stored on a telephone service provider's equipment prior to the intended recipient dialling into their voice mail box to listen to the message.

Under the existing Act, it is essential to know when a particular communication has completed its passage over a telecommunications systems in order to determine whether or not accessing/intercepting the communication is prohibited. Law enforcement agencies are required to obtain an interception warrant to access communications that have not completed their passage. However, if a communication has completed its passage, a different means of lawful access, such as a search warrant, may be used.

The proposed new clauses concerning stored messages are intended to clarify the existing law to provide certainty regarding when a stored communication is still passing over a telecommunications system and hence when an interception warrant is necessary.

The proposed amendments provide that stored communications are passing over a telecommunications system until after they have been read/accessed by the intended recipient (or a person authorised by the intended recipient), or have been delivered to equipment that the intended recipient could use to read/access same without using a telecommunications system to do so. This should ensure that an interception warrant is required to access messages stored on a service provider's equipment until after the message has been read/accessed by the intended recipient (or a person authorised by the intended recipient) or has been delivered to their equipment (e.g. computer, mobile phone handset, etc). After that time, the communication is no longer passing over telecommunications system and therefore if a copy of the message has been left stored on the service provider's equipment, LEAs are permitted to access the stored copy without obtaining an interception warrant. Instead, they may use another means of lawful access, such as a search warrant, applicable to the service provider's or the recipient's premises/equipment.

It may be asked why an interception warrant is not required to access all messages stored on a service provider's equipment, whether or not they have been received by the intended recipient. EFA understands that the government's objective in differentiating between stored messages that have, and have not, been received is to ensure that law enforcement agencies are not unduly hampered in undertaking investigations into criminal activity.

In the case of email for example, as the government has previously said, if all messages stored on an ISP's equipment were deemed to be still passing over a telecommunications system, then criminals could intentionally keep all their email stored on an ISP's server (instead of sending it from, or downloading it to, their own computer) so that LEAs would not be able to access those messages without an interception warrant. As interception warrants can only be obtained in relation to investigation of serious and specified criminal offences, LEAs would not be able to gain access to stored messages when investigating other types of crimes. Further, interception warrants are only available to specified LEAs, not to all police forces or other types of LEAs. However, when messages are sent from the sender's own computer, or downloaded to the intended recipient's computer, LEAs have long been able to obtain access to same with a search warrant allowing access to messages stored on the sender's or recipient's computer (similarly they can obtain access to correspondence stored in a filing cabinet). Hence the government apparently wishes to ensure that it is clear that LEAs are able to use a search warrant to access messages (no longer in transit) that have been stored on an ISP's equipment instead of on the sender or recipient's computer.

EFA considers the proposed amendments provide the most appropriate balance between telecommunications users' privacy and the legitimate needs of law enforcement agencies. We understand that the amendments concerning stored messages do not change the law, they clarify the law to any extent that the current wording of same is insufficiently clear in relation to stored communications. In this regard, then Attorney−General, Daryl Williams, stated in a media release dated 18 December 2001 that:

> "At present, an agency with a valid search warrant cannot access e−mail communications unless they have been read, or otherwise consciously dealt with, by the intended recipient."

In other words, at that date an *interception* warrant was required to access such messages and the relevant sections of the Act have not been amended since then.

However, EFA's support for the currently proposed changes is conditional on our understanding of several aspects being correct and on additional amendments being made to close a significant loophole in the proposed amendments. These matters are discussed below.

4.3 Interpretation of Particular Clauses re Stored Communications

Some wording in the proposed provisions regarding stored communications has resulted in questions being directed to EFA concerning interpretation. EFA's interpretation of these is set out below. EFA supports the provisions if our understanding of same, below, is correct.

4.3.1 Voice over Internet Protocol (VoIP)

Section 10 of Schedule 1 of the Bill states:

> "*Delayed access message services − access to stored communications*
>
> (5) In this section, a *delayed access message service* is a means by which a communication intended for a person can be:
>
> > (a) submitted without the person being in direct contact with anyone submitting the communication; and
> > (b) subsequently accessed by the person (whether or not other persons might also be able to access it);

> but does not include a service for the carriage of communications by way of voice over Internet protocol."

The Explanatory Memorandum states that the reference to VoIP is for the avoidance of doubt. EFA assumes this is intended to address an issue raised by EFA in 2002. The amendments proposed at that time would have enabled stored communications to be accessed without an interception warrant and therefore there was an issue of whether VoIP calls would have been able to be and allowed to be intercepted during the fraction of time VoIP data packets are stored during passage. EFA understands that the specific exclusion of VoIP from the definition of a "delayed access message service" is to ensure there is no doubt that VoIP calls are to be treated the same as ordinary telephone calls under the interception legislation, that is, an interception warrant will be necessary to access any communication at any point in time that is made using VoIP.

4.3.2 Interception during access by intended recipient

Section 10 of Schedule 1 of the Bill states:

> "(6) In this section, a *stored communication* is a communication that:
>
> > (a) has been submitted using a delayed access message service; and
> > (b) is stored on equipment.
>
> (7) For the purposes of this section, a stored communication that is intended for a person (the *intended recipient*) is taken not to be passing over a telecommunications system:
>
> > (a) when it is accessed by or with the authority of the intended recipient; or ..."

The use of the word "when" in 7(a) above appears to give rise to two different interpretations of intent, one consistent with the apparent overall intent of the amendments, and one that is not.

If a stored communication is not "passing over a telecommunications system" "when it is accessed" by the intended recipient, then it appears that it would not be illegal for a third party to intercept the communication when (during the time that) it is being accessed by the intended recipient. EFA assumes that is **not** the correct interpretation in the context.

EFA interprets "when" to mean at the exact time the intended recipient accesses a stored message for the purpose of instructing the service provider's system to transit the message over the telecommunications system to their computer or telephone handset etc so that they can read or listen to it. In our view, once the message commences its passage from the place of temporary storage to the intended recipient's equipment it is clearly a communication passing over a telecommunications system and therefore any third party intercepting that communication (without an interception warrant) would be engaged in illegal interception.

EFA considers that given the overall intent expressed in the Explanatory Memorandum, it is fairly unlikely that a court would interpret the provision in a less protective manner than the foregoing paragraph. Nevertheless, EFA considers the intent of Clause 7(a) should be addressed and clarified during Parliament's consideration of the Bill.

4.4 Interception and Backup of Communications for the Purpose of Disaster Recovery

In EFA's analysis, the proposed amendments in relation to delayed access message services will place carriers and carriage service providers/ISPs in breach of the Act if they have a disaster recovery strategy in place that includes, for example, recording/copying messages delayed during passage onto backup tapes or disks for the purpose of potential disaster recovery. The action of recording/copying such messages will constitute prohibited interception of a communication passing over a telecommunications system, i.e. a contravention of subsection 7(1). The Bill should be amended to deal with this situation.

Furthermore, it appears that in the event of an LEA obtaining a warrant (whether or not an interception warrant) to access such messages stored on disaster recovery backup tapes or disks, a court may find the information to be inadmissible evidence because the copies of the messages came into existence as a result of unlawful interception in the first place. In addition, irrespective of the court's decision in relation to admissibility of evidence, it appears an aggrieved party (i.e. one of the participants to the unlawfully intercepted communication/s), could take civil action against the carrier/carriage service provider (and relevant employees) seeking remedial relief under Section 107A of the Act in respect of the unlawful interception.

These issues are discussed in more detail below together with related recommendations.

4.4.1 Illegal interception by service providers who backup delayed messages

Section 6(1) of the Act, as to be amended by the Bill, defines 'interception' as follows:

> "(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, recording [defined in the Act to include copying], reading or viewing, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.

In relation to knowledge, even if ISPs (and voice mail providers) have made their own customers (recipients) aware that they intercept and record delayed messages, the sender, who is a person making the communication, does not necessarily know that an ISP at the receiving end is intercepting and recording their communications. In this regard, some of the approx. 600 Australian ISPs make copies of messages during passage for the purpose of disaster recovery while others do not. See for example ISP responses to the Australian Communication Authority's Consumer Information Form. As at March 2004, the ACA's web site provides responses from approx. 50 ISPs. A sampling of those responses shows that Netspace, UQ Connect and Alphalink do not intercept and make backup copies of email communications, while Telstra Bigpond, iHug and Westnet do. Responses from some ISPs, for example, OzEmail and Optus, do not make clear whether or not they make backup copies of email.

Section 7(1) of the Act states:

> "(1) A person shall not:
> (a) intercept;
> (b) authorize, suffer or permit another person to intercept; or (c) do any act or thing that will enable him or her or another person to intercept;
> a communication passing over a telecommunications system."

Breach of Section 7(1) above is punishable on conviction by imprisonment for a period not exceeding 2 years (Section 105). In addition, Section 107A makes civil remedies available to participants in communications that have been intercepted in contravention of Section 7(1).

The proposed amendments to the Act make clear that a stored message is "a communication passing over a telecommunications system" until after it has been accessed/read by the intended recipient or delivered to equipment that the intended recipient can use to access it without using a telecommunications system to do so.

It therefore seems clear that a carrier/carriage service provider/ISP employee who routinely records/copies messages delayed and stored during passage from the equipment on which the messages were automatically received to a backup tape/disk for the purpose of potential disaster recovery will be engaging in illegal interception unless an exception to the s.7(1) prohibition on interception applies.

EFA considers it extremely doubtful that any existing exemption would be applicable. In our analysis, the only remotely possible exemptions are contained in s.7(2) and s.6(2). These are discussed below.

Section 7(2) of the existing Act provides that the offence set out in s.7(1) does not apply to or in relation to:

> "(a) an act or thing done by an employee of a carrier in the course of his or her duties for or in connection with:
>
> > (i) the installation of any line, or the installation of any equipment, used or intended for use in connection with a telecommunications service; or
> > (ii) the operation or maintenance of a telecommunications system;
> > ...
>
> where it is reasonably necessary for the employee to do that act or thing in order to perform those duties effectively;"

The above exception is not applicable to the act of copying communications that are delayed and temporarily stored while passing over a telecommunications system. The copying is not necessary for the operation or maintenance of a telecommunications system (telecommunications network) − the telecommunications system will continue to operate, or could cease operating, whether or not communications passing over it are routinely copied onto a separate storage device. Furthermore, if the exception was deemed to be applicable to recording/copying messages temporarily stored during passage, it would also be applicable to listening to and recording ordinary voice calls during passage, contrary to the Government's and Parliament's specific intent in 1995 as outlined below.

As Committee members are likely to be aware, the "reasonably necessary" component of s.7(2) exception was introduced into the Act in 1995 in direct response to the Casualties of Telecom cases ("CoT cases") where the AUSTEL inquiry found that Telecom had intercepted and taped customer telephone calls. The amendment to s.7(2) was enacted to tighten up the exceptions to the prohibitions on interception by a carrier employee in the course of his or her duties. More information about those 1995 amendments is contained in Committee's Report on the *Telecommunications (Interception) Amendment Bill 1995*.

As stated in the Committee's report, in response to the CoT cases Telecom prepared internal guidelines. These made clear that intercepting calls for operation and maintenance purposes was only permitted for brief periods for fault investigation, for example, listening in to check whether a connection had been made or that line/voice quality was of an adequate standard. The guidelines provided that extended voice monitoring could not take place without the customer's consent. Subsequently, the Australian Communications Industry Forum ("ACIF") developed an Industry Guideline − ACIF G517:1998 Monitoring of Communications for Network Operation and Maintenance. The ACIF Guideline is similar to the 1995 Telecom guidelines in relation to intercepting voice calls but also addresses non−voice recording. It provides that, in a case where the customer is identifiable, "non−voice recording may be undertaken to assist in the diagnosis or substantiation of faults or operation or maintenance of the network" only when the customer's consent to recording has been obtained.

It seems clear that the s.7(2) exception does not, and was not intended to, extend to routinely recording/copying communications passing over a telecommunications system and also that it is not perceived to do so by the members of the industry involved in production of the Telecom and ACIF guidelines referred to above.

Section 6(2) of the Act contains an exemption permitting participant monitoring in very narrowly limited circumstances. It states:

> "(2) Where a person lawfully on premises to which a telecommunications service is provided by a carrier, by means of any apparatus or equipment that is part of that service:
>
> > (a) listens to or records a communication passing over the telecommunications system of which that service forms a part, being a communication that is being made to or from that service;
> > (b) listens to or records a communication passing over the telecommunications system of which that service forms a part, being a communication that is being received at that service in the ordinary course of the operation of that telecommunications system; or
> > (c) listens to or records a communication passing over the telecommunications system of which that service forms a part as a result of a technical defect in that system or the mistake of an officer of the carrier;
>
> the listening or recording does not, for the purposes of this Act, constitute the interception of the communication."

The above exemption does not apply to interception by carriers or carriage service providers/ISPs themselves. It applies to interception conducted on premises to which a telecommunications service is provided by a carrier, that is, the premises of senders and recipients of communications. It obviously does not apply to, for example, ISPs copying messages delayed during transit because, among other things, the equipment that would be being used to record/copy the communication is not part of a telecommunications service being provided to the ISP by a carrier. The telecommunications service, that is, the email service, is being provided by the ISP. (It should be noted that the s.6(2) exemption dates back to the days when all telecommunications services were provided by Telstra and was intended to provide, for example, an exemption for listening in to a telephone call using an extension handset in a home when that handset was part of the telephone service provided by Telstra. The applicability of the exemption is widely regarded as being extremely uncertain in the modern telecommunications environment and hence unsuitable for being

relied on by persons wishing to avoid imprisonment. The uncertainty of the s.6(2) exception is discussed in more detail in section 5 the Telecommunications Interception Policy Review paper prepared by the Cth Attorney General's Department in 1999.)

EFA is of the view that if the Bill is passed without amendments to address the situation concerning copying of messages delayed during their passage over a telecommunications system onto backup tapes or disks for the purpose of disaster recovery, those ISPs who choose to do so are very likely to be found in breach of the Act. This could occur either as a result of criminal proceedings or civil action taken by participants to unlawfully intercepted communications. The same situation would apply to telephone service providers who make backup copies of voice mail messages delayed during passage. Whether or not that is the government's and Parliament's intent should be clarified.

In addition, our analysis of the existing Act and Bill undertaken in considering the effects of the proposed amendments, has drawn to our attention that service providers who are currently intercepting and storing delayed messages on backup storage devices are quite probably in breach of the existing Act.

We consider that at present it is fairly unlikely that a court would convict in a criminal prosecution given the high standard of proof necessary and the beyond reasonable doubt requirements combined with the lack of clarity in the existing Act concerning communications delayed and stored during passage. However, whether a court would find contravention of the Act in a civil action is more open to question, particularly given the civil remedies were introduced into the Act in direct response to the Casualties of Telecom cases.

Regardless of the current situation, in our view if the proposed amendments concerning delayed access message services are enacted, thereby removing any doubt as to whether temporarily stored messages are passing over a telecommunications system, there will be a significantly greater probability of ISPs being found in contravention of the Act for intercepting and copying such messages onto other storage devices.

Of equal concern is the potential for courts to find evidence, obtained from backup storage devices and submitted by law enforcement agencies, to be inadmissible because the information was obtained by unlawful interception.

EFA considers it is essential that the Bill be amended to provide certainty to carriers/carriage service providers and the courts concerning interception of communications for the purpose of disaster recovery. It should not be left to the courts to attempt to guess whether the Parliament intended such interception to be legal or illegal, nor what means of access is lawfully available to LEAs.

We consider that rather than outlawing the practice of intercepting and making backup copies of delayed communications, which is a value added service some service providers choose to provide to their customers, it is preferable to strictly regulate the practice to ensure telecommunications users' privacy is adequately protected. It must be remembered that the practice affects not only the service provider's own customers but many other people who communicate with such a service provider's customers. A vast number of communications that are copied onto backup storage devices are sent by people who are not customers of the service provider who intercepts those communications.

Suggested clauses to amend the Bill in relation to the above issues, and those discussed in the section below, are provided later herein.

4.4.2 Access to intercepted messages copied onto disaster recovery backup storage devices

If the Bill is amended to permit service providers to intercept messages during passage over a telecommunications system in order to record/copy same onto backup tapes or disks for the purpose of disaster recovery, EFA considers the Bill should also be amended to ensure that an interception warrant is required to access such messages. An example situation is as follows.

Emails messages for a particular recipient are received on an ISP's equipment on Monday. The intended recipient does not access or download their messages until Tuesday. On Monday night, the ISP makes backup copies of all messages delayed and temporarily stored during passage. Although the intended recipient downloads their messages on Tuesday and the messages are thereby deleted from the ISP's mail server equipment, copies of the intercepted messages that were made by the ISP before they were delivered remain on backup storage devices in the possession of the ISP.

Furthermore, some ISPs could consider nightly backups inadequate for the purpose of disaster recovery and may make frequent backups during the day. As a result potentially every message that has passed over the ISP's system will have been intercepted and copied onto a backup storage device. EFA does not know whether any of the ISPs who currently make backups of undelivered email do so more than once a day. Whether or not backups are currently made more frequently than daily, such a practice could commence at any time.

The same situation as above would apply to telephone service providers who make backup copies of voice mail messages and text (e.g. SMS) messages temporarily stored during passage.

As outlined above, the proposed amendments intended to protect messages temporarily stored during passage would be a very weak form of protection unless there is also prohibition on access to messages that have been intercepted during passage and recorded/copied onto backup storage devices.

EFA considers that copies of messages that would exist only because of an exemption to the prohibition on interception for the purpose of disaster recovery should not be permitted to be disclosed or used for any purpose.

EFA recommends that, if the Bill is amended to permit interception of delayed messages in order to record/copy same onto disaster recovery backup storage devices, the Bill also be amended to prohibit access to, use and disclosure of messages stored on such devices for any purpose other than disaster recovery. Otherwise, at the very least, an interception warrant must be required.

Suggested clauses to amend the Bill are provided below.

4.4.3 Recommended amendments re interception for disaster recovery purpose

EFA recommends that the Bill be amended to include clauses substantially similar in intent to those suggested in **bold text** in the extract of the Bill below. There may be other ways in which the Bill or Act could be amended to achieve the same intent. However, in view of the short period given to the Committee to conduct its inquiry, we have chosen to place our concerns and suggestions that come readily to mind before the Committee at the earliest opportunity, rather than firstly spending substantially more time analysing the existing Act and Bill with a view to determining whether there may be alternative and better ways of amending the Bill or Act.

The intent of our suggested clauses suggested is, as discussed earlier herein, to:

- make clear that undelivered communications that are intercepted and copied onto a backup storage device for the purpose of enabling disaster recovery are still passing over a telecommunications system while stored on that backup storage device, and therefore an interception warrant is necessary to access such communications (proposed item (6A) below); and
- that an employee of carrier who copies communications stored during passage onto a backup storage device or restores the backup copies onto the system equipment on which they were received is not, in so doing, engaging in unlawful interception (proposed items 7(aa) and 7(ab) below). Note that in these two proposed clauses, the the word "when" is intended to mean *when* an employee engages in the act of recording a communication. It is *not* intended to mean that *while* an employee is recording a communication another person could also legally intercept/record the same communication. The word "when" has been used for consistency with the government−proposed amendments which, as discussed earlier herein in relation to item 7(a), have given rise to questions concerning the correct interpretation of "when". If EFA's interpretation of the government's use of "when" (discussed earlier herein) is *not* correct, then that word would also not be suitable for use in proposed items 7(aa) and 7(ab) below.

(Suggested amendments are shown in **bold text** below.)

Delayed access message services − access to stored communications

(5) In this section, a *delayed access message service* is a means by which a communication intended for a person can be:

(a) submitted without the person being in direct contact with anyone submitting the communication; and
(b) subsequently accessed by the person (whether or not other persons might also be able to access it);
but does not include a service for the carriage of communications by way of voice over Internet protocol.

Note: Some common examples of delayed access message services are e−mail services and voice mail services.

(6) In this section, a *stored communication* is a communication that:

(a) has been submitted using a delayed access message service; and
(b) is stored on equipment.

(6A) In this section, for the avoidance of doubt, *equipment* includes a back up storage device on which recordings of communications submitted using a delayed accessed message service are stored for the purpose of enabling disaster recovery.

[Note: The existing Act states:

- *equipment* means any apparatus or equipment used, or intended for use, in or in connection with a telecommunications network, but does not include a line.

- *telecommunications network* means a system, or series of systems, for carrying communications by means of guided or unguided electromagnetic energy or both, but does not include a system, or series of systems, for carrying communications solely by means of radiocommunication.]

(7) For the purposes of this section, a stored communication that is intended for a person (the *intended recipient*) is taken not to be passing over a telecommunications system:

(a) when it is accessed by or with the authority of the intended recipient; or

(aa) when an employee of a carrier in the course of his or her duties in connection with disaster recovery records a stored communication onto a backup storage device for the purpose of enabling disaster recovery; or

(ab) when an employee of a carrier in the course of his or her duties in connection with disaster recovery records a communication that has been stored on a backup storage device onto equipment on which the intended recipient can access the stored communication; or

(b) when it is accessed by another person at any time after it is accessed by or with the authority of the intended recipient, so long as it is accessed by the other person without using a telecommunications service or any other form of remote access, unless the use of the telecommunications service or the other form of remote access, as the case may be, is merely for the purpose of, or an incidental result of:

(i) turning on equipment; or
(ii) obtaining power required to operate equipment; or
(iii) any other action prescribed by regulations for the purposes of this subparagraph; or

(c) when it is accessed by another person using:

(i) any or all of the equipment which the intended recipient could have used to access the stored communication; or
(ii) any or all of the equipment mentioned in subparagraph (i) in combination with other equipment;
so long as it is accessed by the other person without using a telecommunications service or any other form of remote access, unless the use of the telecommunications service or the other form of remote access, as the case may be, is merely for the purpose of, or an incidental result of:
(iii) turning on equipment; or
(iv) obtaining power required to operate equipment; or
(v) any other action prescribed by regulations for the purposes of this subparagraph.

▲ Go to Contents List

5. Extension of interception warrants to "cybercrime" offences

Section 4 of Schedule 1 of the Bill proposes to extend the definition of "Class 2 offences" to include a number of so−called "cybercrimes" in State and Territory legislation, thereby extending the availability of interception warrants to investigation of such offences. The particular offences listed in the Bill are:

> "(b) section 308C, 308D, 308E, 308F, 308G, 308H or 308I of the Crimes Act 1900 of New South Wales;
> (c) section 247B, 247C, 247D, 247E, 247F, 247G or 247H of the Crimes Act 1958 of Victoria;
> (d) a provision of a law of a State (other than New South Wales or Victoria) that corresponds to a provision covered by paragraph (a), (b) or (c);
> (e) a provision of a law of a Territory that corresponds to a provision covered by paragraph (a), (b) or (c);
> (f) section 440A of The Criminal Code of Western Australia."

Although the above offences are referred to in the Bill as "cybercrimes" they are in fact computer offences that may be committed without using a telecommunications system to commit the offence. Furthermore, while Class 2 offences are generally specified offences that carry a maximum of 7 years imprisonment, a number of the proposed Class 2 offences carry a maximum penalty of only 1, 2, 3 and 5 years imprisonment. In addition, some of these offences are ones where a person can be found guilty of the offence "even if committing the serious computer offence concerned is impossible". For example, Section 308F of the Crimes Act 1900 of New South Wales states:

> "308F Possession of data with intent to commit serious computer offence
>
> (1) A person who is in possession or control of data:
>
> > (a) with the intention of committing a serious computer offence, or
> > (b) with the intention of facilitating the commission of a serious computer offence (whether by the person or by another person), is guilty of an offence.
> > Maximum penalty: Imprisonment for 3 years.
>
> (2) For the purposes of this section, "possession or control of data" includes:
>
> > (a) possession of a computer or data storage device holding or containing the data or of a document in which the data is recorded, and
> > (b) control of data held in a computer that is in the possession of another person (whether the computer is in this jurisdiction or outside this jurisdiction).
>
> (3) A person may be found guilty of an offence against this section even if committing the serious computer offence concerned is impossible.
> (4) It is not an offence to attempt to commit an offence against this section.

As can be seen from the above, a person could be in possession or control of illegal data without using a telecommunications system to obtain or retain such possession or control. Furthermore they could be found guilty of breaching s308F of the NSW Act even if it is impossible to use the data

to commit a serious computer offence. s308G of the NSW Act is similar in that regard, as are several sections of the Victorian Act.

EFA considers criminal offences such as the above to be ridiculous and a matter for law reform. EFA therefore also opposes extension of the interception warrant regime to investigation of such offences.

EFA considers the Bill should be amended to limit the availability of interception warrants to computer offences defined in State and Territory legislation to the following:

- offences that carry a maximum penalty of 7 or more years imprisonment and where it is possible to commit the offence; and
- in the case of offences carrying a lesser penalty, investigation only of instances of the offence where a telecommunications system is used to commit the actual offence and only in instances where it is possible to commit the serious criminal offence.

EFA also observes that although it is proposed to enable interception warrants to be issued where a person is suspected of a computer offence involving *less than* a maximum of 7 years imprisonment (including when it is impossible to commit the serious computer offence), an interception warrant is not available when a person is suspected of dealing in armaments and firearms (nor various other crimes) unless the offence involves a maximum of 7 years imprisonment and also "involves 2 or more offenders and substantial planning and organisation; and involves, or is of a kind that ordinarily involves, the use of sophisticated methods and techniques; and is committed, or is of a kind that is ordinarily committed, in conjunction with other offences of a like kind". EFA considers it would be appropriate to similarly limit interception warrants to computer offences involving those additional components.

We note that the existing Act already enables interception warrants to be obtained in relation to computer offences set out in Part 10.7 of the Commonwealth Criminal Code, which are similar to the State/Territory offences listed in the Bill. Offences against Part 10.7 were made Class 2 offences under the *Telecommunications (Interception) Act 1979* when the *Cybercrime Bill 2001* was rushed through Parliament in the wake of September 11. EFA considers the *Telecommunications (Interception) Act 1979* should be amended to limit the applicability of interception warrants to Commonwealth computer offences in the same way as outlined above in relation to State/Territory computer offences.

▲ Go to Contents List

6. Interception of calls made to ASIO

The proposed amendments would exclude from the definition of interception the act of listening to, recording, reading or viewing communications to publicly−listed ASIO numbers (by a person lawfully engaged in duties relating to the receiving and handling of calls to that number).

EFA is opposed to this amendment in the absence of any apparent legitimate reason for the change. The Explanatory Memorandum provides no information as to why the change is considered necessary. EFA understands that ASIO, like other government departments and businesses, would already be permitted to listen to or record calls made to their own telephone numbers provided the participants in the communication are notified of the listening or recording, for example, by an announcement at the beginning of a telephone call. When such knowledge is provided, the recording or listening does not constitute 'interception' under the existing Act. EFA sees no reason

why callers to ASIO numbers should not be notified at the time of the call that the communication is being monitored or recorded.

▲ Go to Contents List

7. Removal of requirement for ASIO to notify telecommunications carrier of interception

The Explanatory Memorandum states:

> "Subsection 15(1A) [of the existing Act] imposes an obligation on the Director−General of Security to cause the Managing Director of a carrier [includes carriage service provider/ISP] to be informed of the issue of a telecommunications interception warrant to [ASIO] by the Attorney−General and to be provided with a certified copy of the warrant. The inclusion of [new] paragraph (ba) has the effect of limiting the requirement to notify the Managing Director and to provide a copy of the warrant to cases where the execution of the warrant will involve the taking of action by the carrier or its employees. The requirement to notify a carrier of the issue of a warrant by the Attorney−General, and to provide a copy of that warrant, is unnecessary in cases where effecting interception will not require action on the part of the carrier. The amendment therefore removes the requirement to notify in those cases."

EFA is opposed to this amendment. We consider the existing requirement to notify the Managing Director of a carrier (includes carriage service provider/ISP) serves as an accountability check and in the event of problems occurring within the carrier's system during execution of a warrant, enables the carrier to take the matter up with ASIO. EFA sees no legitimate reason why a carrier's Managing Director should not be in a position to know who has been interfering with their telecommunications system.

▲ Go to Contents List

8. Conclusion

EFA considers the objective of the Bill in relation to protecting delayed access message services provides a reasonable degree of protection to Internet and other telecommunications users and that the clarification provided by the relevant amendments is certainly needed. However, unless the Bill is amended to address the practice of intercepting and recording messages onto backup storage devices, which may or may not currently be in contravention of the Act, and also to provide protection for such stored messages, the protection provided by the currently proposed amendments will be very weak and therefore inadequate.

The proposed extension of interception warrants to so−called 'cybercrime' offences is far too broad. The Bill should be amended to exclude computer offences that do not involve the use of telecommunications system and that carry penalties less than the generally applicable seven years for interception warrant availability.

EFA also considers the proposed amendments in relation to ASIO should be deleted from the Bill in the absence of provision of any legitimate reason for the need for these changes.

▲ Go to Contents List

References

Telecommunications (Interception) Amendment Bill 2004

- Text of Bill
- Explanatory Memorandum

Telecommunications (Interception) Act 1979

Senate Legal and Constitutional Committee, Report on the *Telecommunications (Interception) Amendment Bill 1995*

Australian Communications Industry Forum, Industry Guideline − ACIF G517:1998 Monitoring of Communications for Network Operation and Maintenance.

Attorney General's Department, Telecommunications Interception Policy Review, May 1999

▲ Go to Contents List