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

6 August 2004

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

Email: legcon.sen@aph.gov.au

Dear Mr Bailey

Inquiry into the provisions of the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004*

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

Yours sincerely

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA) Submission

To: Senate Legal &Constitutional Legislation Committee
Re: *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004*

6 August 2004

Contents:

Introduction

Firstly, we express our serious concern regarding the exceedingly short time frame (one week) the Committee was given to inquire into the provisions of this lengthy and complex Bill and the resultant twenty−four hour period available to members of the public for preparation and lodgement of submissions. EFA considers that Senate Committees serve an important and essential function in reviewing proposed legislation and that Committee members, their staff and the public should be given a reasonable period of time to consider proposed legislation. One week is not, in our view, reasonable. It is also not adequate to enable the public to have faith in the Committee system and processes.

Obviously this submission has been prepared in one day. EFA was only able to prepare this submission so quickly because we had analysed an exposure draft earlier this year.

In April 2004, EFA sent a submission to the Attorney−General's Department in response to their request for comments on the *Exposure Draft of the Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004* and associated Explanatory Notes. A copy of that submission is attached and is referred to herein as our "April submission".

Many of the numerous issues and concerns raised in our April submission were addressed and resolved to EFA's satisfaction by the Attorney−General's Dept prior to introduction of the proposed legislation into Parliament on 24 June 2004. The *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004* ("the Bill"), introduced into Parliament on 4 August, appears to be the same as the June Bill (apart from the removal of provisions concerning suicide material, which are now in another Bill).

While the majority of comments in our April submission are not relevant to the Bill, we have attached a copy of that submission so that if there are any proposals to revert to provisions similar to

those in the April Exposure Draft, the Committee will have information readily available regarding EFA's reasons for objecting to the previously proposed provisions. (Clause numbers referred to in our April submission refer to the numbers in the Exposure Draft which are slightly different from those in the Bill.)

The following provisions in the Exposure Draft were changed in a manner that appears to satisfactorily resolve the concerns raised by EFA:

- ISP Liability, Internet Users' Rights and Criminal Justice
  − lack of necessary defences for ISPs (resolved by new section 474.13)
- Definitions of Types of Material
  − requirement to take into account the same matters (merit, character of material, etc) as in the C'th Classification Act (resolved by new section 473.4).
- Using a carriage service for child pornography/abuse material s474.19/22 (was 474.17/20)
  − clarification of element of intent (resolved by amended paras (1)(a) and (2)).

In the remainder of this submission we discuss provisions of the Bill that we remain concerned about, both those that have not been changed since the Exposure Draft, and those that have been improved but not sufficiently in our view.

▲ Go to Contents List

Using a carriage service to menace, harass or cause offence 474.17 (was 474.16)

This offence replaces s85ZE of the *Crimes Act 1914* and significantly broadens same. EFA is strongly opposed to the proposed changes to the existing offence.

Our April submission outlines our interpretation of the proposed changes, which we believe to be correct following a telephone discussion with representatives of the A−G's Department, followed by details of our concerns as to the effect of these changes.

Since the Exposure Draft, changes including the addition of two new sections are a significant improvement and resolve some aspects of the concerns raised in our April submission. These new sections are:

- Section 473.4 "Determining whether material is offensive" containing provisions suggested in our April submission; and
- Section 474.13 "Use of a carriage service" which should eliminate the previous high potential for ISPs to be menaced (by legislation) into becoming the nation's censors and conduct police which we believe would have resulted in due process not being available to 'accused' persons.

However, we remain opposed to the proposed new offence because:

- unlike existing s85ZE of the Crimes Act, the proposed new offence enables a person to be found guilty even when no person has in fact been menaced, or harassed, or been caused offence; and

- unlike existing s85ZE(1)(b), the proposed offence applies to all 'Internet content', i.e. including web pages, etc. The existing offence re offensive use excludes 'Internet content'

and therefore applies only to 'ordinary email' (which is excluded from the definition of 'Internet content' in the *Broadcasting Services Act 1992* ("BSA")). This situation was explictly intended by the government in 1999 and is a complete reversal of that policy position.

EFA is implacably opposed to any offence the same as or similar to s85ZE(1)(b) being applicable to "Internet content" as defined in the BSA. The existing offence already enables prosecution of a person who makes telephone call/s or sends email message/s to another person that reasonable persons would regard in all the circumstances as offensive. Existing s85ZE(1)(b) serves a legitimate purpose and its coverage must not be extended to Internet content.

EFA is also strongly opposed to changes to the existing provisions of s85ZE in relation to menacing or harassing use. The existing offence already enables prosecution of people who menace or harass another person. As discussed in our April submission, obviously the aim of the proposed offence is to facilitate criminal prosecution of Internet users, and especially political activists, in relation to speech and conduct that does **not** menace or harass another person, and that also does **not** promote, instruct or incite in matters of violence or crime. As set out in our April submission, speech that does do so can already be dealt with under existing laws.

EFA is also opposed to the penalty for this offence. The penalty for the existing narrower offence is one year, in the Exposure Draft it was to be increased to two years (which EFA did not oppose), but in the Bill it has been increased to three years. EFA suspects it is not mere coincidence that three years is also the period applicable to a 'relevant offence' in the *Surveillance Devices Bill (No. 2) 2004* for which police will be able to obtain a surveillance device warrant (and in some circumstances use such devices without a warrant). EFA does not believe that surveillance device warrants should be available to LEAs investigating such broadly defined suspected offences as those in proposed s474.17. Questions arise as to whether the overall objective is to enable LEAs to covertly surveil political activists without justifiable cause. The penalty should be no more than two years.

▲ Go to Contents List

Interception devices 474.4 (was 474.6)

Although the majority of comments in our April submission related to the first TI Bill this year (which is different from the latest TI Bill), we remain of the view that the definition of 'interception device' is insufficiently narrowly tailored to avoid catching equipment that should not be illegal to sell, possess, etc.

In addition, the related Crimes Act Regulations which are to continue to apply, and may be relevant to the above concern, refer to ss6(3) of the *Telecommunications (Interception) Act 1979*. However, there is no ss6(3) of that Act.

Further information in relation to the above matters and need for amendment is contained in our April submission under the heading "474.6 Interception devices".

▲ Go to Contents List

Wrongful delivery of communications 474.5 (was 474.7)

Para (2) of this section was not in the Exposure Draft and appears to have been added to resolve an issue raised in our April submission. While the addition of this exception from criminal responsibility is a significant improvement and resolves part of the problem, we remain concerned that the offence is insufficiently narrowly defined and could catch conduct that should not be a criminal offence. For example, if <johnsmith@companyname.com.au> leaves the company and the employer redirects mail to that person to <janeblack@companyname.com.au> it appears the employer would be in breach of the law if the employer is not the person operating the carriage service, unless the employer can obtain John Smith's consent to the redirection. An employer would not always be able to obtain consent depending, for example, on the circumstances of a person's termination of employment.

▲ Go to Contents List

Definition of 'Carriage Service'

The comments in our April submission concerning whether or not the offences are intended to apply to the use of a private (not public) network still apply. We have not had time to read the latest Explanatory Memorandum to ascertain whether a related explanatory note has been added, as suggested, or not.

▲ Go to Contents List

Possessing, controlling, producing, supplying or obtaining child pornography material for use through a carriage service 474.20 (was 474.18)

We remain concerned (see April submission) regarding whether or not the rules of double jeopardy apply in relation to this offence or whether a person could be prosecuted for possession with intent of use in commission of an offence under C'th law and also simple possession under State/Territory law. If the rules of double jeopardy do not apply to such a situation, EFA is opposed to s474.20 and the similar s474.23.

▲ Go to Contents List

Defences in respect of child pornography/abuse material s474.21/24 (was 474.19/22)

These two sections have been significantly revised since the Exposure Draft and we have not had the opportunity to closely analyse the differences. Our previous major concern regarding the lack of defence for ISPs has been resolved by new Section 474.13. Other revisions to these two sections also appear, generally speaking, to probably be an improvement.

We remain of the view that a defence should be available for persons reporting spam containing illegal material to the Australian Communications Authority ("ACA"). Alternatively if people should not report such spam to the ACA, this should be made publicly known by the ACA. This

may be covered by s474.21(2) but if it is then the question arises as to why there is a separate defence for reporting material to the Australian Broadcasting Authority (s474.21(4)).

Go to Contents List

Conclusion

While the Bill is a significant improvement over the Exposure Draft, further amendments are necessary. Proposed Section 474.17 should be changed to the same as existing s85ZE and amendments made to other sections to address matters discussed above.

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.

Go to Contents List

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 April 2004

Assistant Secretary
Criminal Law Branch
Attorney−General's Department
Robert Garran Offices
National Circuit
BARTON ACT 2600

Email: telecomoffences@ag.gov.au

Dear Sir

Exposure Draft of the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004*

Please find attached submission from Electronic Frontiers Australia Inc. in relation to the above draft Bill.

EFA appreciates the opportunity to make a submission and we would be pleased to provide further information or discuss any issues raised on request.

Yours faithfully

Irene Graham
Executive Director
Electronic Frontiers Australia Inc.

Electronic Frontiers Australia Inc. (EFA)

Submission to Attorney−General's Department

re Exposure Draft of the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004*

12 April 2004

This is a submission in response to the Exposure Draft of the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill 2004* and associated Explanatory Notes issued for public comment by the Attorney−General's Department on 14 March 2004.

Contents:

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.

▲ Go to Contents List

Introduction

EFA has reviewed the draft Bill and associated Explanatory Notes in the context of the existing provisions of the *Criminal Code Act 1995* concerning criminal responsibility (e.g. physical and fault elements of offences).

We observe that a number of the proposed offences are revised versions of existing offences in the *Crimes Act 1914* and the majority of these appear to us to be of the same intent and effect as the existing offences. As such they do not appear to raise issues of concern and therefore are not mentioned in this submission.

Overall, we consider most of the proposed offences have been drafted in a manner that is reasonably easy to understand and are appropriately adapted to serve a legitimate end. This is a welcome change in comparison with some similar pre−existing laws in Australian jurisdictions.

However, we do have major concerns about some proposed offences and, in addition, consider some other offences and/or definitions require an improvement in clarity. These matters are addressed later in this submission.

We take this opportunity to commend the Criminal Law Branch of the Attorney−General's Department for issuing an exposure draft of the Bill along with detailed Explanatory Notes. The Notes have been of significant assistance in comprehending this large and complex draft Bill. We also wish to record our thanks to several representatives of the Criminal Law Branch for their willingness to respond to several questions about the draft Bill which was also very helpful.

▲ Go to Contents List

Offences

Subdivision B−Interference with telecommunications

474.6 Interception devices

We note that this offence is to replace existing s85KB of the Crimes Act and is intended to prohibit the same type of devices. However we consider that either the definition of an interception device needs to be changed, or the related Regulations and s6(2) of the *Telecommunications (Interception) Act 1979* ("TI Act") need to be amended, in the light of modern telecommunications technologies and the government's proposed amendments to the TI Act.

We understand from discussion with representatives of the Attorney−General's Department ("A−G's Department") that this section was drafted prior to introduction into Parliament of proposed amendments to the *Telecommunications (Interception) Act 1979* ("TI Act") concerning delayed access messages passing over a telecommunications system, which are currently under re−consideration and revision by the government. We also understand that the A−G's Department intends to review the proposed interception device offence in the draft Bill when the proposed amendments to the TI Act are finalised and we offer the following observations and comments with a view to assisting that process.

The term 'interception device' is defined in proposed Section 474.4 as follows:

> ***interception device*** means an apparatus or device that:
> (a) is of a kind that is capable of being used to enable a person to intercept a communication passing over a telecommunications system; and
> (b) could reasonably be regarded as having been designed:
> (i) for the purpose of; or
> (ii) for purposes including the purpose of;
> using it in connection with the interception of communications passing over a telecommunications system; and
> (c) is not designed principally for the reception of communications transmitted by radiocommunications.
> Terms used in this definition that are defined in the *Telecommunications (Interception) Act 1979* have the same meaning in this definition as they have in that Act.

The above definition includes devices and apparatus that can be used for both legal and illegal purposes. It is clear that is the intent of the definition from other provisions in the existing and proposed laws.

Proposed Section 476.6 states:

> *(1) A person is guilty of an offence if:*
> *(a) the person:*
> *(i) manufactures; or*
> *(ii) advertises, displays or offers for sale; or*
> *(iii) sells; or*
> *(iv) possesses;*
> *an apparatus or device (whether in an assembled or unassembled form); and*
> *(b) the apparatus or device is an interception device.*
> *Penalty: Imprisonment for 5 years.*

In conjunction with the definition of 'interception device', the above makes it an offence to sell or possess etc. any device or apparatus that can be used to intercept a communication passing over a telecommunications system, irrespective of whether the interception is legal or illegal.

Some exceptions to the offence are included in s474.6(2) and (3) of the draft Bill, for example, in relation to a person's duties involving interceptions that are not in contravention of the TI Act.

However, none of the exceptions including those in the existing Regulations (which are discussed later herein) appear to be applicable to the use of modems, mobile phones, telephone handsets and other devices and apparatus by persons accessing their own email and stored voice mail messages, that can also be used by other persons to engage in illegal interception.

While the sale, possession etc of such devices may or may not be technically illegal now, it appears it would be illegal under proposed s474.6 of the draft Bill if amendments to the TI Act, substantially similar to those that were in the *Telecommunications (Interception) Amendment Bill 2004* ("TI Bill"), are also enacted.

The TI Bill was said by the A−G's Department to, among other things, clarify the existing law to ensure it is clear that "delayed access messages" (i.e. stored communications such as email, SMS and voice mail messages) are passing over a telecommunications system until they are received or otherwise accessed by the intended recipient. The TI Bill included the following:

> (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
> (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 ...

Para 7(a) above was apparently included in the TI Bill because otherwise a person accessing their own email or stored voice messages would be engaging in illegal interception. Therefore, any device or apparatus that is used for the purpose of accessing stored communications is an 'interception device' as defined in the draft Bill because the definition does *not* exclude devices designed or used for legal interceptions. It appears modems and mobile phones etc, would be an interception device because they certainly "*could reasonably be regarded as having been designed for...purposes including the purpose of using it in connection with the interception of communications passing over a telecommunications system*", given they are commonly used for such a purpose, that is, to access temporarily stored messages passing over a telecommunications system.

With regard to exceptions in the Regulations, the Explanatory Notes state that the existing Regulations in relation to s85ZKB of the Crimes Act will continue to apply. Those regulations include sale, possession, etc "*for a purpose related to interception of communications that is not in contravention of subsection 7 (1) of the Telecommunications (Interception) Act 1979 because of subsection 6 (3) or 7 (2) of that Act*".

However, there is no subsection 6(3) in the TI Act (according to the copies on Scaleplus and Austlii). We question whether the reference to subsection 6(3) is meant to refer to subsection 6(2) of the TI Act. However, even if it does and is amended to say that, we do not consider this would be adequate to resolve the problem discussed above. The lack of certainty about the applicability of s6(2) of the TI Act (participant monitoring) is discussed in the Telecommunications Interception Policy Review paper prepared by the C'th Attorney General's Department in 1999 and the relevant aspects of the law have not changed since then. As stated in that paper:

> "Such a test might have been relatively easily administered in an environment where there was only one carrier since it could have been assumed that any apparatus or equipment that was supplied by the carrier was part of the service. Its application in an environment where there is more than one carrier and an unlimited number of service providers is far less clear. ... The consequences of a mistaken analysis could be quite serious. In addition to the possibility of a criminal conviction for an illegal intercept, the Act has, since 1995, also provided civil penalties for a breach of the prohibition against interception (s.107A)."

Furthermore, the above paper appears to discuss primarily telephone services and in our view it is even more problematic to apply the test in s6(2) in relation to Internet services such as email and related devices and apparatus. In addition it only applies to listening to and recording, while proposed amendments to the TI Act extend the definition of interception to reading and viewing.

In summary, unless amendments are made to the draft Bill or the Regulations, the provisions appear to place people who sell, possess, etc. a modem or mobile phone etc. in breach of the Criminal Code Act. Even if that would not currently be the result, it appears it will if amendments to the TI Act concerning delayed access messages, substantially similar to those in the TI Bill 2004, are enacted.

Obviously such an outcome would be ludicrous and would not be enforced. However, the examples serve to demonstrate the breadth of coverage and the high probability of difficulty of determining whether devices or apparatus that may be developed, or proposed to be developed, in the future would be illegal.

▲ Go to Contents List

474.7 Wrongful delivery of communications

The draft states:

> 474.7 A person is guilty of an offence if:
> (a) a communication is in the course of telecommunications carriage; and
> (b) the person causes the communication to be received by a person or carriage service other than the person or service to whom it is directed.
> Penalty: Imprisonment for 1 year.
>
> *communication in the course of telecommunications carriage* means a communication that is being carried by a carrier or carriage service provider, and includes a communication that has been collected or received by a carrier or carriage service provider for carriage, but has not yet been delivered by the carrier or carriage service provider.

This offence is almost identical to s85ZD of the Crimes Act which was probably written before ISPs and Internet communications existed and appears not to have been reviewed in light of modern telecommunications technologies.

The offence appears to criminalise services that some customers of ISPs would want and that should not be illegal to provide. For example, a company that does not have its own domain name may arrange for an ISP to provide them with email addresses for each of their employees in the form "johnsmith@ispname.com.au", "janeblack@ispname.com.au", etc. When John Smith leaves the company, the employer may request the ISP to redirect communications addressed to "johnsmith@ispname.com.au" to the replacement employee, e.g. bobjohnson@ispname.com.au. In doing so, the ISP would be causing communications to be received by a person other than the person to whom they are directed, i.e. a 'wrongful delivery' offence. An ISP cannot be expected to know of arrangements between employers and employees concerning redirection of email and the law should not prohibit this type of service from being available to ISPs' customers.

With regard to the remarks in the Explanatory Notes that:

> 60. The proposed offence will not apply to the diversion of communications, such as telephone calls or emails, within an organisation's internal telecommunications

> system. The phrase 'communication in the course of telecommunications carriage' does not cover such communications
>
> 37. The phrase does not apply to a communication that is within the internal telecommunications system of an organisation, for example a telephone call that has entered an organisation's PABX system. Such a communication has already been delivered by a carrier or carriage service provider, so is no longer being carried by a carrier or carriage service provider.

We do not see how a call that is still in progress can be 'no longer being carried' by a carrier/CSP. The caller is still on the phone, so the originating carrier/CSP is obviously still carrying the call. We consider the definition needs amendment such as removing the words "and includes" and clarifying that it is intended to refer only to communications that have not been "delivered".

However, it is also not clear when an email communication would be regarded as having been "delivered" by a carrier/CSP. Unlike a telephone call which is addressed/delivered to a carriage service (telephone service/number) not a person, an email message is addressed to a person not a carriage service. The addressee may use a variety of different carriage services to collect their email from time to time (e.g. a carriage service supplied to their home, or their office, or to a hotel, etc). Hence it appears that an email can not be regarded as having been delivered by a carrier/CSP until it is received by the person − as the terminating carriage service varies. This seems to indicate that an employer who redirected email received by their mail server to an employee other than the addressee would commit a wrongful delivery offence. We are uncertain whether or not the foregoing would be the situation and we therefore consider either the Bill or the Explanatory Notes need to clarify this matter so that the law can be understood by persons who are required to comply with same.

We recognise that the phrasing of the proposed offence is substantially the same as an existing offence. However, old offences are less likely to be enforced in new circumstances where it seems doubtful that the original intent was applicable to such circumstances. The proposed repeal of the existing offence and enactment of an almost identical offence would remove any doubt as to whether the offence is intended to be applicable to relatively new types of carriage services. It therefore has more potential to result in unintended consequences and undesirable prosecutions.

▲ Go to Contents List

Subdivision C−Offences related to use of telecommunications

Definition of Carriage Service

We observe that the proposed definition of "carriage service" in the Dictionary would, on its face, include private telecommunications services that are not connected to the public network. This definition, in conjunction with the proposed deletion of the words "supplied by a carrier" from existing offences in the Crimes Act, results in proposed offences apparently being applicable to use of any carriage service.

For example, the offence proposed to replace s85ZE of the *Crimes Act 1914* (offensive use, etc) applies to use of any carriage service, whereas s85ZE applies only to use of a carriage service "supplied by a carrier" (which includes a CSP).

The reason for this change is not apparent in the Explanatory Notes and it may appear to some readers that the Commonwealth proposes to criminalise various types of use of a carriage service

that is a private (not public) telecommunications system.

EFA considers whether or not that is the intent should be made clear, at the least, in the Explanatory Memorandum to the final version of the Bill. In this regard, the A−G's Department informed a Senate Committee in March 2004 (Submission No. 6D re TI Bill 2004) that in 2001 in relation to the Cybercrime Bill there "was doubt whether the Commonwealth could seek to regulate a computer network within an organisation that uses exclusively lines provided by the organisation". As there has been no change to the Constitution, EFA assumes there is still doubt. Therefore to avoid doubt in relation to the proposed offences, the government's intent should be made clear in the Explanatory Memorandum.

The above applies to all replacement and also new offences in the draft Bill, not only the one replacing s85ZE.

▲ Go to Contents List

474.14 Using a carriage service to make a threat

These proposed new offences prohibit using a carriage service, to make to another person, a threat to kill a person or a threat to cause serious harm to a person with the *intention* to intimidate or instil fear in the person to whom the threat is made that it will be carried out.

We understand that the existing definitions of harm, serious harm, threat, etc, in the Dictionary in the Criminal Code Act will apply to this offence.

As these two offences are limited to making a threat *to another person* as distinct from making public non−specific threats against the public at large or groups or classes of people, and relevant words are carefully defined, and requires the prosecution to prove intention to instil fear in the person to whom the threat is made, it appears to be sufficiently narrowly tailored to serve a legitimate end without resulting in broad restrictions on speech.

▲ Go to Contents List

474.15 Using a carriage service for a hoax threat

This is a proposed new offence, similar to an existing offence concerning use of a postal service.

As this offence requires the prosecution to prove intention to induce a false belief that an explosive, or a dangerous or harmful substance or thing, has been or will be left in any place, it appears to be sufficiently narrowly tailored to serve a legitimate end without resulting in broad restrictions on speech.

▲ Go to Contents List

474.16 Using a carriage service to menace, harass or cause offence

This offence replaces s85ZE of the *Crimes Act 1914* and significantly broadens same. EFA has major concerns about the proposed changes.

We outline below our interpretation of the proposed changes, which we believe to be correct following a telephone discussion with representatives of the A−G's Department, followed by details

of our concerns as to the effect of these changes.

Menacing or harassing use

Outline of proposed offence

The existing offence, s85ZE states:

> (1) A person must not intentionally use a carriage service supplied by a carrier:
> (a) with the result that another person is menaced or harassed; or
> ...
> Penalty: Imprisonment for 1 year.

The proposed offence states:

> (1) A person is guilty of an offence if:
> (a) the person uses a carriage service; and
> (b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, menacing [or] harassing ...
> Penalty: Imprisonment for 2 years.

Both the existing and proposed offence apply to 'Internet content', (i.e. web pages etc as well as ordinary email).

Unlike s85ZE, the proposed new offence enables a person to be found guilty even when no person has in fact been menaced or harassed. The Explanatory Notes make clear that this proposed change is not an accidental result of drafting. The notes state:

> "145. The proposed offence is broader than existing subsection 85ZE(1)...because it removes the requirement that the recipient be in fact menaced or harassed and replaces it with an objective standard. The proposed offence provides that reasonable persons must regard the use of the carriage service, given all the circumstances, as menacing, harassing or offensive. This allows community standards and common sense to be imported into a decision on whether the conduct is in fact menacing, harassing or offensive."

Both the existing and proposed offence comprise two physical elements that are required to be proven. It is a change to the second of these elements that broadens the offence.

The first physical element is conduct that is use of a carriage service. Both the existing and proposed offence require intention to use to be proven. (Neither the existing or proposed offence requires intention to menace or harass another person.) As stated in the Explanatory Notes:

> "148. The existing offence in section 85ZE explicitly provides that the offending conduct, of using a carriage service, must be intentional. The reference to intention is not included in proposed section 474.16, because by application of the default fault elements of section 5.6 of the Criminal Code the fault element of intention will automatically apply to this **physical element of conduct**. This means that a person must intentionally use the carriage service to be found guilty of the offence." (emphasis added)

In the existing offence, the second physical element is *a result* of the conduct − that another person is menaced or harassed. This requires proof of recklessness concerning the result that another person was in fact menaced or harassed. This element, that the result occur, is not part of the proposed offence.

Instead, in the proposed offence, the second physical element is *a circumstance* of the conduct − that the use was done "in a way...that reasonable persons would regard as being, in all the circumstances menacing or harassing". This requires proof of recklessness concerning what 'reasonable persons' would think. As stated in the Explanatory Notes:

> "149. The fact that the use of the carriage service occurs in a way that reasonable persons would regard as being, in all the circumstances, menacing, harassing or offensive constitutes a circumstance in which the offending conduct must occur. By application of the default fault elements in section 5.6 of the Criminal Code, the fault element of recklessness will apply to a **physical element of an offence that is a circumstance**. 'Recklessness' as it applies to a circumstance is defined in section 5.4 of the Criminal Code." (emphasis added)

Section 5.4 of the Criminal Code states:

> (1) A person is reckless with respect to a circumstance if:
> (a) he or she is aware of a substantial risk that the circumstance exists or will exist; and
> (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

Issues

As shown above, the proposed offence contains no requirement that the person have intent to menace or harass another person, nor that any other person is in fact menaced or harassed, only that the person has been reckless with regard to a possibility that "reasonable persons" would regard the use as being menacing or harassing.

EFA is strongly opposed to the removal of the requirement that another person be in fact menaced or harassed.

The replacement of that requirement with, in effect, the opinion of "reasonable persons" about what is menacing or harassing appears to be the only aspect of the draft Bill that seeks to give effect to the Government's announcement in August 2003 that:

> "*People using the Internet to advocate or facilitate violent protests, for example by spreading information on methods of violently disrupting international meetings and attacking police officers protecting such gatherings, including those using the Internet to harass or menace others are amongst those who could be prosecuted under the new offences.*"

The reason for the proposed change to s85ZE(1)(a) is no doubt the result of complaints by two Ministers about the speech of some anti−WTO protesters on two or three web sites in September 2002. However, if the complained about material could not have been dealt with under existing law, then in EFA's view it is certainly not deserving of criminal prosecution.

In relation to existing law and the WTO protest material:

- Firstly, under existing s85ZE(1)(a), which applies among other things to Internet content, person/s could have been prosecuted if a police officer (or any other person) had been menaced or harassed by or as a result of the material on the web pages and was prepared to appear in court and state that. Given apparently either no police officer was prepared to state that, or the Director of Public Prosecutions did not consider it in the public interest to prosecute, EFA considers there was no speech deserving of criminal prosecution.
- Secondly, material that "promotes, instructs or incites in matters of violence or crime" can already be classified "Refused Classification" and such material has been prohibited Internet content under Schedule 5 of the *Broadcasting Services Act 1992* since 1 January 2000. According to media reports (e.g. *ABA clears anti−WTO websites*, ABC News, 31 Oct 2002), the Australian Broadcasting Authority ("ABA") found the material was not prohibited content, therefore it evidently did not promote or instruct or incite in matters of violence or crime. EFA assumes the ABA would have referred the material, in such a publicly and politically controversial instance, to the Office of Film and Literature Classification ("OFLC") although the ABA is not required to do so if the sites were hosted outside Australia. If the ABA did refer the material to the OFLC, then according to the OFLC's online classification database, the material was apparently classified M (3 items so classified for the ABA on 4 October 2002) or classified G or PG.

Obviously the aim of the proposed offence is to facilitate criminal prosecution of Internet users, and especially political activists, in relation to speech and conduct that does **not** menace or harass another person, and that also does **not** promote, instruct or incite in matters of violence or crime. As set out above, speech that does do so can already be dealt with under existing laws.

EFA is strongly opposed to changes to the existing provisions of s85ZE in relation to menacing or harassing use. The existing offence already enables prosecution of people who menace or harass another person.

Offensive use

Outline of proposed offence

The existing offence, s85ZE states:

> (1) A person must not intentionally use a carriage service supplied by a carrier:
> ...
> (b) in such a way as would be regarded by reasonable persons as being, in all the circumstances, offensive.
> Penalty: Imprisonment for 1 year.
> (2) Paragraph (1)(b) does not apply to the use of a carriage service to carry Internet content.

The proposed offence states:

> (1) A person is guilty of an offence if:
> (a) the person uses a carriage service; and
> (b) the person does so in a way (whether by the method of use or the content of a communication, or both) that reasonable persons would regard as being, in all the circumstances, ...offensive.
> Penalty: Imprisonment for 2 years.

We note that it is not proposed to change the physical elements of this offence, nor the fault elements of intention and recklessness that are required to be proved, which are the same as those applicable to menacing and harassing use.

However, unlike existing s85ZE(1)(b), the proposed offence applies to all 'Internet content', i.e. including web pages, etc. The existing offence re offensive use excludes 'Internet content' and therefore applies only to 'ordinary email', which is excluded from the definition of 'Internet content' in the *Broadcasting Services Act 1992* ("BSA"). The Explanatory Notes (para 146) make clear that this proposed change is not an accidental result of drafting.

Issues

The proposed change is a direct reversal of the Federal Government's 1999 decision to amend Section 85ZE to explicitly exclude Internet content from coverage by s85ZE(1)(b) on commencement of the Federal Government's Internet censorship laws on 1 January 2000.

To date the Federal Government has claimed that Section 85ZE of the Crimes Act is inadequate to deal with illegal online content and that is why the government considered specific Internet censorship legislation was necessary. In this regard, according to the government there was (and therefore must still be) doubt about the Commonwealth's Constitutional powers in relation to the applicability of s.85ZE to Internet content. For example, a FAQ concerning on−line content regulation issued by the Department of Communications has, since it was first issued in mid 1999, stated (Q 1.2):

> "Some prosecutions in relation to online content have been initiated under section 85ZE. However, successful prosecutions under this provision have been on the basis of guilty pleas and therefore its application to online services has not been fully tested by a court."

It could not have been tested since 1 January 2000 and EFA finds it extremely disturbing that the government now apparently wishes to start testing it by way of a virtually identical offence in the Criminal Code.

EFA assumes that the previous successful prosecutions under s85ZE on the basis of guilty pleas would most likely have concerned child pornography material. The proposed offence is not necessary to deal with such material since the draft Bill contains specific offences concerning child pornography material and child abuse material. It also contains specific offences concerning threats and hoaxes.

In the absence of any information or indications to the contrary, EFA considers it reasonable to assume that the reversal of the Government's position arises from:

- highly controversial classification decisions in recent years, such as the OFLC Classification Board's decision to ban the film *Ken Park*;
- media reports that some Internet users had downloaded the film *Ken Park* from overseas web sites;
- the majority of State and Territory governments declining to create laws 'complementary' to the Federal Government's Internet censorship regime to enable criminal prosecution of Internet users and content providers who distribute or download material deemed "offensive" by the Commonwealth.

The Commonwealth Government has consistently claimed that the Commonwealth law deals with material that is "offensive". For example the DCITA FAQ states: "The Commonwealth legislation regulates the activities of ISPs and ICHs. The second tier of the regulatory framework will be uniform State and Territory legislation...regulating the activities of persons who create **offensive** material, who transfer such material onto or from the Internet, or who use such material". (emphasis added)

This offensive material, i.e. "prohibited content" under the Commonwealth law, includes material that is or would be classified R18+ (i.e. unsuitable for minors) and X18+ (i.e. depicting non−violent sexually explicit activity between consenting adults).

It seems beyond doubt that the proposed offence is intended, among other things, to enable the ABA to refer Internet content that has been classified R18+ or X18+ or "Refused Classification" to Federal police for prosecution of the content provider. To date, it has been considered a decision for State and Territory Governments as to whether or not their censorship laws enable criminal prosecution of Internet users.

Furthermore, the proposed offence is so broad it would cover not only distribution of "offensive" material but also **access to** such material. As such the offence could in effect criminalise access to material that is not illegal to possess offline under the States' and Territories' censorship laws.

In addition to the types of material referred to above, we observe that the Explanatory Notes claim the proposed offence would cover "use that vilifies persons on the basis of their race or religion". EFA considers it highly inappropriate to attempt to deal with such matters by way of laws criminalising "offensive" use of a carriage service. Matters of vilification should be dealt with under laws of general application and we note that HREOC has previously ordered removal of Internet content found to be in breach of the C'th Racial Hatred Act. If the government considers existing laws of general application are inadequate or that HREOC does not have sufficient powers, then the government should seek to amend any such deficiencies in those laws and powers, but not by way of vague provisions in the Criminal Code, nor only in relation to use of the Internet and telephone services.

Furthermore, we note that when an identical offence in relation to use of a postal service was introduced in 2002 (*Criminal Code Amendment (Anti−Hoax and Other Measures) Bill 2002*), the government stated in the Explanatory Memorandum that in practice the offence would cover material containing "offensive language" and "sexual connotations". Such an offence may be appropriate in relation to letters sent to a person in some circumstances; it is not appropriate for broad application under criminal law to web pages, mailing lists or chat rooms.

In summary, EFA is implacably opposed to any offence the same as or similar to s85ZE(1)(b) being applicable to "Internet content" as defined in the BSA. The existing offence already enables prosecution of a person who makes telephone call/s or sends email message/s to another person that reasonable persons would regard in all the circumstances as offensive. Existing s85ZE(1)(b) serves a legitimate purpose and its coverage must not be extended to Internet content.

We recognise that the probable response/reaction to our concerns set out above is that the proposed offences are only likely to result in successful convictions in cases of extremely offensive material/conduct due to the need for a jury find guilt proven beyond a reasonable doubt.

However, such an argument does not address the fact that the proposed offence readily facilitates selective enforcement and victimisation; nor the cost and trauma to individuals in defending themselves against a criminal charge; nor that the mere threat of criminal prosecution chills freedom

of expression. Moreover, EFA believes that in the vast majority of instances there will be no opportunity for a jury to make a decision because the draft Bill contains provisions that appear intended to threaten and menace Internet service providers into becoming the nation's censors and conduct police, thereby achieving a large part of the objective of the provisions without due process being available to 'accused' persons. This issue is addressed in detail in the following section.

ISP Liability, Internet Users' Rights and Criminal Justice

ISP Criminal Liability

Section 474.16 (menacing, harassing, offensive use) of the draft Bill purports to offer a defence to ISPs and ICHs in relation to use of their services by another person. It states:

> (2) A person is not criminally responsible for an offence against subsection (1) if the person:
>
> > (a) is an Internet service provider (within the meaning of Schedule 5 to the Broadcasting Services Act 1992) or an Internet content host (within the meaning of that Schedule);
> > and
> > (b) is acting solely in the person's capacity as an Internet service provider or Internet content host; and
> > (c) is not aware of the method of use or the content of the communication by which an offence under subsection (1) is committed by another person.
> > Note: A defendant bears an evidential burden in relation to the matter in this subsection, see subsection 13.3(3).

This defence is totally unsatisfactory.

Firstly, the Explanatory Notes (para 151) make quite clear the drafters consider an ISP could be prosecuted in relation to use by someone else, e.g. one of their customers. If that is in fact so, then a telephone company can also be prosecuted in relation to someone else making menacing, harassing or offensive phone calls, or sending illegal images to a mobile phone. Why is no defence provided for a telephone call carrier/service provider in the draft Bill and why has there been no defence for carriers in existing s85ZE? If ISPs are to be required to terminate a customer's Internet access service when they are "made aware" the customer is engaging in illegal use, then Telstra, Optus and other telephone service providers should surely be required to disconnect a customer's telephone service when they are "made aware" the customer is making menacing or harassing calls or sending offensive images to another person's mobile phone.

Furthermore, if an ISP can be regarded as the person using a carriage service to commit an offence when in fact someone else has engaged in the illegal use, it would appear parents could be charged in relation to use of their computer/Internet access account by their adult (or minor) children and an employer could be charged in relation to use by an employee. Provisions of the Criminal Code concerning body corporate criminal responsibility may be applicable to employers in such an instance, however, we question the situation concerning parents and other people who allow someone else to use a carriage service, given the intent to provide a defence for ISPs in similar circumstances.

Secondly, the defence provision requires an ISP or ICH to in effect prove a negative, that they were not aware. Generally speaking, EFA does not consider it appropriate for criminal law to reverse the

evidential burden and especially not to require a person to prove they did **not** know or do something. In the case of ISPs it is already commonly known that they are not aware, in the normal course of events, of the content of information passing through their system and so the mere fact that a person is an ISP should be adequate to meet the evidential burden (balance of probability), therefore there should not be any need to place an evidential burden on an ISP in the first place. The prosecution should be required to prove that the ISP was aware in the specific instance, that is, the fault element of knowledge should apply because ISPs' normal business practice comprises intention to transmit/make available material. The same situation applies to many Internet content hosts, as one example, those who are in the business of providing merely web hosting server space for their customers.

Thirdly, the intention to threaten ISPs and ICHs into becoming the nation's censors is the direct opposite of Government's 1999 decision concerning ISPs and ICHs in relation to the Internet censorship regime.

In this regard the Explanatory Notes to the draft Bill state:

> 152. ...The defence for ISPs and ICHs will not be available in situations where they are made aware of offending use of a carriage service (whether due to the method of use or the content of a communication) that occurs through a service they provide, and they facilitate that offending use by allowing their systems to continue to be used for this purpose. **Possible action that could be taken by ISPs and ICHs so as not to facilitate use of a carriage service by another person that breaches proposed subsection 474.16(1) includes an ISP ceasing to provide Internet services to that person or an ICH ceasing to host a particular website containing content that breaches the proposed offence.** (emphasis added)

The above is in stark contrast to the situation applicable to ISPs and ICHs under Schedule 5 of the BSA, which does not require ISPs to take action until they are notified by the ABA that the content is in breach of the law (or that is very likely to be and is being referred for classification by OFLC Classification Board). The reasons for the Government's decision in that regard are stated in the Explanatory Memorandum to Schedule 5 of the BSA:

> "...online service providers are primarily carriers of material (although in some limited instances they act as content providers and to that extent will be subject to proposed State and Territory legislation). Material subject to a complaint would not generally be originated by the service provider. **It would therefore appear unreasonable to expect services providers to adjudicate complaints about material for which they are not responsible. Industry has a valid concern about the capacity for individual service providers to undertake complaints resolution − in terms of time, cost, and expertise. They are reluctant to make decisions about the classification of content, particularly where the material may be illegal and an error of judgement on the service provider's part could leave them open to sanctions under the proposed framework, or litigation by aggrieved customers.** [emphasis added]
> ...
> ...[T]he Government has decided ... that service providers will not be the first point for complaints from the public about online content hosted on their services; complaints will be made directly to the ABA."

The proposed offence or related defence must be amended so that ISPs are not required to determine whether conduct or speech is illegal. It is completely unreasonable to in effect require ISPs to decide

whether or not particular conduct or speech would be regarded by "reasonable persons" in all the circumstances as menacing, harassing or offensive. Furthermore, ISPs cannot possibly know whether a person's use was intentional and reckless nor whether guilt could be proven beyond a reasonable doubt. Neither ISPs or their lawyers are qualified to make such determinations, nor can they even be expected to make a fair and reasonable determination when the ISP risks criminal prosecution for a wrong guess.

Internet Users' Rights and Criminal Justice

EFA is extremely concerned that requiring ISPs to make such determinations will result in Internet users having their Internet access service terminated and/or their content taken down when they have not in fact infringed the law.

The provisions leave the door wide open to vexatious complaints and victimisation. One of many example scenarios is as follows.

Betty contacts John's ISP and informs them that he is distributing, and/or accessing, illegal material on the Internet, and/or that he is menacing or harassing her via the Internet (whether he is or not is beside the point). The ISP has been "made aware" that their carriage service is being used by John to commit an offence. The ISP would not necessarily have any means of ascertaining whether the allegation against John is true or not. There are many ways an Internet user can use the Internet without evidence of such activity being logged or recorded by the systems under the control of the ISP who provides them with Internet access. Therefore, even if the ISP checked their logs, they cannot be sure that John is not using their carriage service in an illegal manner. The ISP has two choices:

1. Give John the benefit of the doubt. In this instance it may transpire that Betty also informed the police of John's illegal activities and also informed them that she had made the ISP aware of John's use. The police investigate and find the allegation to be true. In such circumstances the ISP has no defence and can be prosecuted themself for allowing John's use to continue after they had been made aware.
2. Terminate John's Internet access service. In this instance, if John was not doing anything illegal (Betty made a vexatious complaint about John because for example she hates him), he cannot prove that he was not, and in any case he has no means of appeal.

In short, the provisions of the draft Bill effectively compel ISPs to terminate a user's access in response to **any** allegation of offensive, menacing or harassing use of their service. EFA does not believe any ISP would be prepared to risk criminal prosecution themself. As a result, Internet users will be denied due process of the law and they will not have a means of appeal.

It may be claimed that a person in situation (2) above could take action against the ISP for breach of contract. However, the ISPs Terms and Conditions of service/use may allow them to terminate an account for any reason whatsoever at their discretion. Even if the ISP's T&Cs were in breach of consumer protection laws, it is contrary to normal principles of fairness and justice for an individual to have to take costly (or any) court action against an ISP to regain services that were unfairly terminated due to criminal law that gives ISPs no choice but to terminate access. Further, it is questionable whether a court would find in favour of the customer given the customer can not prove that they did not use the ISP's service in an illegal manner.

In summary, EFA is highly disturbed that this draft Bill raises many of the same issues and concerns as those that were addressed and largely resolved in relation to the Internet censorship regime, that is, Schedule 5 of the BSA. While EFA is a critic of that regime, it does treat both ISPs and Internet

users fairly in relation to the matters raised above. ISPs are not required to be the nation's censors and users can be reasonably well assured that decisions of the ABA and OFLC will be fair and impartial as they are not at risk of criminal prosecution themselves. Furthermore if the user/content provider does not agree with the ABA/OFLC decision, they at least have the right to appeal as a person aggrieved by the classification decision.

The draft Bill must be amended to result in arrangements substantially similar to those in the BSA in relation to ISP liability and users' rights.

▲ Go to Contents List

473.2−3 Definitions of possession, control, supplying, obtaining of data

Section 473.2 (Possession or control of data or material in the form of data) states:

> A reference in this Part to a person having possession or control of data, or material that is in the form of data, includes a reference to the person: ...
> (b) having possession of a document in which the data is recorded; or ...

The term "document" should be defined to state whether it refers only to an electronic document, or whether it include a paper document. It should also be clarified in the similar item (b) of Section 473.3 (Producing, supplying or obtaining data or material in the form of data).

▲ Go to Contents List

474.12 Definitions of Types of Material

In relation to the definitions of "child pornography material" and "child abuse material" we note that the Explanatory Notes state:

> 116. The qualification requiring that reasonable persons must regard the material, given all the circumstances, as offensive allows community standards and common sense to be imported into a decision on whether material is offensive. A range of factors should be taken into account in determining whether certain material in fact comes within the definition, including whether the material has any literary, artistic or educational merit, or whether the material appears in a medical or scientific context.

We consider the definitions should be amended to incorporate a requirement to take into account any literary, artistic or educational merit of the material and its general character including whether it is of a medical, legal or scientific character (the same as the C'th Classification Act), or otherwise the legislation should include a specific requirement that the court inform the jury that they are required to take such factors into account.

Apart from the above, in our view the definitions of "child pornography material" and "child abuse material" are appropriately narrowly tailored to ensure that offences would only apply to material that is already probably illegal to possess under State and Territory laws. We commend the effort apparently undertaken to define the material in detail rather than use vague terms such as "child pornography" that appear in some State legislation and mean different things to different people. In our view the definitions assist towards an improved level of certainty by members of the public and law enforcement agencies, concerning the type of material intended to be proscribed.

Go to Contents List

474.17 Using a carriage service for child pornography material

The draft Bill states:

> *(1) A person is guilty of an offence if:*
> *(a) the person uses a carriage service to:*
> *(i) access material [includes display and any other output from a computer; copying or moving material; and execution of a program]; or*
> *(ii) cause material to be transmitted to the person; or*
> *(iii) transmit material; or*
> *(iv) make material available; or*
> *(v) publish or otherwise distribute material; and*
> *(b) the material is child pornography material.*
> *Penalty: Imprisonment for 10 years.*
> *(2) To avoid doubt, the following are the fault elements for the physical elements of an offence against subsection (1):*
> *(a) intention is the fault element for the conduct referred to in paragraph (1)(a);*
> *(b) recklessness is the fault element for the circumstances referred to in paragraph (1)(b).*
> *Note: For the meaning of intention and recklessness see sections 5.2 and 5.4 of the Criminal Code.*

We note para (2)(a) has been included for the avoidance of doubt, however, we consider it is insufficiently clear. It seems to us the matters listed in (i) to (v) of para (1) could be regarded as either conduct or the result of the conduct of using a carriage service. The Explanatory Notes indicate para (2)(a) has been included to ensure that 1(a)(i) to (v) are treated as conduct so that intention is required. We are concerned however that para (2)(a) can be read as referring only to the first line of 1(a) (use of a carriage service) and not to the remainder of 1(a). We therefore recommend that para (2)(a) be made clearer by changing it to "intention is the fault element for the conduct referred to in paragraph (1)(a)(i) to (v) inclusive".

In relation to proof an offence was committed, the Explanatory Notes state:

> 157. Subsection 474.17(2) provides that intention applies as the fault element for the conduct listed in paragraph 474.17(1)(a) and recklessness is the fault element for the circumstance that the material is child pornography, provided in paragraph 474.17(1)(b). These are the default fault elements that would have applied if this subsection was not included, by application of section 5.6 of the Criminal Code. 'Intention' and 'recklessness' are defined in sections 5.2 and 5.4 of the Criminal Code, respectively.

However, neither the Draft Bill nor Explanatory Notes make clear how it will be decided whether or not material is in fact child pornography. The definition of the material contains a qualification requiring that reasonable persons must regard the material, given all the circumstances, as offensive. EFA would be highly concerned if this aspect involving the views of "reasonable persons" would be determined by solely a magistrate or judge. We understand however that due to Section 4G of the *Crimes Act 1914* (Cth) these offences are indictable offences and therefore must be heard by a jury (unless the defendant consents to waive their right to trial by jury).

Further, EFA is under the impression that the rules of double jeopardy would apply in relation to prosecution under the proposed Commonwealth offence and similar existing offences in State/Territory laws. We trust that is correct.

474.18 Possessing, controlling, producing, supplying or obtaining child pornography material for use through a carriage service

We note this offence concerns, among other things, possession and is a preparatory offence intended, generally speaking, to enable law enforcement agencies to take action to prevent commission of the offence of transmitting, making available, etc. We also note that a person would, in principle, also be criminally responsible under State/Territory laws for simple possession. We question whether the rules of double jeopardy apply in such instances or whether a person could be prosecuted for **possession with intent of use in commission of an offence** under C'th law and also **simple possession** under State/Territory law. If the rules of double jeopardy do not apply to such a situation, EFA is opposed to s474.18.

474.19 Defences in respect of child pornography material

Para (3) of s474.19 provides a defence for an Internet service provider in relation to s474.17. This defence is basically identical to that provided in Section 474.16(2) (re menacing, harassing, offensive use) and all issues raised above in relation to s474.16(2) also apply to this section.

In addition, we are concerned that s474.19(3) only provides a defence to ISPs in relation to s474.17 (using a carriage service), and not also s474.18 (possession or control of material). However, defences available to some other types of persons refer to both s474.17 and s474.18. It seems there should also be a defence for ISPs in relation to the preparatory offence in s474.18 (possession or control of material) because ISPs will certainly have possession of material with the intention of transmitting it to another person when, for example, a spammer has sent child pornography material to one of the ISP's customers. Such a material will be in the intended recipient's email box on the ISP's mail server until the ISP's mail server transmits it to the intended recipient (e.g. until the intended recipient downloads their email). Hence it appears that would constitute possession/control by the ISP with the intention of transmitting.

With regard to defences available to other persons, according to the Explanatory Notes:

> 175. ...Paragraph 474.19(6)(a) concerns persons who engage in the offending conduct for the sole purpose of assisting the Australian Broadcasting Authority (ABA) to detect prohibited content in the performance of its functions under the Scheme. An example of a situation in which this defence would apply is where a person makes a complaint to the ABA under the Scheme by emailing an attachment containing child pornography material. A person whose only reason for transmitting such material is to assist the ABA in its functions under the Scheme should not be liable for that conduct.

While a defence is provided in relation to reporting to the ABA, no defence is provided in relation to reporting to police (although that is mentioned in para 156 of the Explanatory Notes). In addition, persons may wish to also report spam containing unsolicited illegal material to the Australian Communications Authority (as referred to in para 172 of the Notes). EFA considers defences should be provided in relation to reporting material to police and the ACA.

▲ Go to Contents List

474.20 Using a carriage service for child abuse material

474.21 Possessing, controlling, producing, supplying or obtaining child abuse material for use through a carriage service
474.22 Defences in respect of child abuse material

As these offences about are almost identical to those about 'child pornography material', all comments made earlier herein in relation to 'child pornography material' also apply to the equivalent provisions about 'child abuse material'.

▲ Go to Contents List

474.23−6 Use of telecommunications to procure or "groom" persons under the age of consent

We have not had sufficient time during the one month consultation period to analyse the complex provisions in s474.23 to s474.26 (inclusive) and therefore we have no comments on the details at this time.

However, we note the statement in the Explanatory Notes that:

> "The Federal Minister for Justice and Customs invites specific comment on the merits of adopting an alternative strategy of imposing a blanket 'age of consent' of 16 years nationally rather than the current proposal to retain a complex 'age of consent' jurisdictional trigger."

We have reviewed the information in the Explanatory Notes in relation to the age of consent issues and we consider it would be better to adopt a blanket 'age of consent' of 16 years nationally. We believe this would minimise jurisdictional problems and difficulties for law enforcement agencies. We also feel it would minimise the potential for individuals who have no intent of breaking the law to inadvertently attract the attention, time and effort of law enforcement agencies simply because they did not even know about the variances in age of consent throughout Australia. While a blanket age can be seen to afford insufficient protection to older persons in some jurisdictions, we are of the view that persons 16 and older are fairly likely to be aware of risks online and therefore at less risk of procurement or grooming than younger persons. The blanket age would enable law enforcement agencies to focus their efforts towards protecting those who are more at risk.

▲ Go to Contents List

474.27 Using a carriage service for suicide promotion material

Although the Explanatory Notes (para 124) claim that the definition of "suicide promotion material" is "consistent with the description of the types of documents (in hard copy) that are prohibited from being imported or exported under the Customs...Regulations", in fact the definition covers vastly more speech.

The Customs Regulations prohibit only speech that concerns the use of a "device designed or customised to be used by a person to commit suicide, or to be used by a person to assist another person to commit suicide", while the definition in the draft bill is:

suicide promotion material means material that, directly or indirectly:
(a) promotes, counsels or incites suicide; or
(b) provides instruction on how to commit suicide.

This definition is so broad it could be used to silence the speech of advocates of laws such as the now demised Northern Territory euthanasia legislation.

The proposed offence also enables the criminal prosecution of a person who accessed such material with the intention of using the information to commit suicide themself. Such people need help and support. Charging them with a criminal offence is more likely to result in them actually committing suicide that achieving anything else.

The Federal Government should have learned by now that Australian laws prohibiting speech on the Internet are incapable of effectively censoring speech and information that is legal in other countries. The proposed legislation will not protect anyone because the same information can be made available by people overseas − anyone who wants to commit suicide will continue to be able to find information on how to do so (in the event that they do not already know), notwithstanding that it would be an offence to access such information. Furthermore, it is notable that the government does not propose to criminalise the use of a postal service for accessing or distributing such information.

Given the above situation, the proposed offence appears to have the primary purpose of silencing the speech of one particular high profile Australian resident, but only in relation to use of the Internet.

The proposed offences concerning "suicide promotion material" should be deleted entirely.

▲ Go to Contents List

Conclusion

In summary, EFA is of the view that:

- Proposed additions to the Criminal Code that change the existing phrasing in s85ZE of the *Crimes Act* (use that is menacing, harassing or offensive) must be deleted from the Bill (other than minor re−phrasing of the first line of s85ZE for the sole purpose of aligning it with standardised phrasing used in the Criminal Code).
- Issues raised above concerning ISP liability, Internet users' rights and criminal justice must be addressed and resolved in a fair and reasonable manner before the proposed Bill is introduced into Parliament. These issues are relevant to all proposed offences (not only proposed changes to s85ZE) where an ISP or ICH could be held criminally responsible for use by someone else.
- All paragraphs included for the avoidance of doubt in relation to the fault element of intention should be made clearer, for example, as discussed above regarding Section 474.17(2).
- Defences should be provided in relation to reporting material to police and the Australian Communications Authority.
- Proposed offences prohibiting speech and reading in relation to information described as "suicide promotion material" should be deleted.
- Definitional issues raised above in relation to interception devices, wrongful delivery of

communications, the terms 'carriage service' and 'document', should be addressed and clarified.

- It would be preferable if the eventual Explanatory Memorandum contained information concerning the applicability of rules of double jeopardy in relation the same/similar offences in Commonwealth and State/Territory legislation.

Finally, while we appreciate the Attorney−General's Department providing a one month period for public comment, we have not had sufficient time/resources to closely analyse some provisions of the draft Bill because there have also been three other Commonwealth Parliamentary and government agency invitations for public comment in the same period concerning issues of interest and concern to EFA. In this submission, therefore, we have addressed matters of the most concern and relevance to EFA's aims and objectives. Our lack of comment on other provisions of the draft Bill therefore should not be regarded as necessarily signifying agreement with provisions on which we have not commented.

▲ Go to Contents List