Electronic Frontiers
AUSTRALIA

PO Box 382, North Adelaide SA 5006
T +61 2 9011 1088 F +61 2 8002 4009
E email@efa.org.au W www.efa.org.au
ABN 35 050 159 188

Committee Secretary
Senate Legal and Constitutional Committee
PO Box 6100
Parliament House
Canberra ACT 2600
Australia

Telecommunications (Interception and Access) Amendment Bill 2009 (Cth)

The Senate Legal and Constitutional Affairs Committee has called for submissions on the Telecommunications (Interception and Access) Amendment Bill 2009 (Cth) (**the Bill**) by 09 October 2009. This Bill proposes to amend the *Telecommunications (Interception and Access) Act 1979* (Cth) (**TIAA**) to allow limited interception of communications for network protection purposes.

Electronic Frontiers Australia Inc. (EFA) welcomes the opportunity to submit comments to the Bill. EFA has a long-standing interest in telecommunications policy in Australia, and seeks to promote a balanced regulatory approach that respects the rights and interests of users and providers of network services.

EFA is a non-profit national organisation representing internet users concerned with on-line freedoms and rights. EFA was established in January 1994 and incorporated under the Associations Incorporation Act (SA) 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 is dedicated to supporting a reasonable telecommunications policy in Australia that balances the needs of carriers and carriage service providers, end users, law enforcement agencies, and other interested parties.

EFA supports the Telecommunications (Interception and Access) Amendment Bill 2009 (Cth) in its current form.

EFA suggests that there are a small number of relatively minor amendments that could be made to the the Bill in order to clarify its operation.

Background issues with exposure draft

EFA lodged a submission with the Commonwealth Attorney-General's Department regarding the exposure draft of the current Bill in August 2009.[1] At that stage, EFA opposed the exposure draft, pointing out that it did not "provide sufficient clarity or adequate protections for the privacy of network users. "[2]

The exposure draft allowed a very broad discretion to network operators to intercept communications in order to monitor compliance with any applicable contractual arrangements between the operator and their subscribers. The previous definition of 'network protection duties' in s 5(1) included monitoring of the content of communications in order to ascertain whether the network was being 'appropriately used'. Because of the broad undefined nature of the term 'appropriately used' and the fact that many AUPs may contain restrictions not on protocols or services that internet users may use but upon the purpose for which those communications are being made, this provision opens the bulk of network communications to potential interception and continuing surveillance.

As the exposure draft was worded, it would have permitted network operators to intercept communications, for example, to determine whether peer-to-peer filesharing traffic was infringing a third party's copyright interests, or to determine whether the network was being used for excessive personal use. This represented, in EFA's view, an unacceptable threat to the privacy of internet users in Australia.

The exposure draft also provided a broad ability for network operators to disclose the substance of intercepted communications to an unlimited group of people for undefined 'disciplinary purposes'. Given the broad definition of 'appropriate use' as discussed above, the potential range of information that is available to be disclosed under this subsection is very large. These provisions radically alter the existing law and presumptions of privacy in network communications. EFA is not aware of any pressing reasons to allow such broad disclosure, and opposed the broad exceptions to the prohibition on intercepting and disclosing telecommunications in the exposure draft.

The current Bill

EFA is pleased to note that the Bill, as introduced to the House of Representatives, addresses all of the EFA's concerns that were raised in the submission to the exposure draft. EFA commends the Attorney-General's Department on achieving a workable legislative exception to the prohibition on interception of telecommunications that allows network operators to perform legitimate network protection duties without unduly burdening the privacy of end users.

Most importantly, the Bill now limits 'network protection duties' for all networks to duties relating to 'the operation, protection or maintenance of the network'.[3] The ability to intercept communications in order to determine whether a network is being 'appropriately used' is now expressly limited to operate only in relation to users of Commonwealth agencies, security authorities, or eligible State authorities.[4]

---

1 Electronic Frontiers Australia, Submission to the Attorney-General's Department, *TIAA Amendments: Computer Network Protection*, 07 August 2009 <http://www.efa.org.au/main/wp-content/uploads/2009/08/20090807-EFA-AGD-TIAA-Computer-Network-Protection.pdf>.

2 Ibid, 2.

3 Telecommunications (Interception and Access) Amendment Bill 2009 (Cth), Schedule 1, cl 1.

4 Telecommunications (Interception and Access) Amendment Bill 2009 (Cth), Schedule 1, cl 1.

The exception to the broad prohibition on interception contained in proposed s 7(2)(aaa) of the TIAA is appropriately limited to persons authorised by the network owner to engage in network protection duties and purposively to interception that is reasonably necessary to perform those duties.[5]

The Bill now provides a much stronger explicit limit on disclosure of information intercepted under proposed s 7(2)(aaa), allowing communication only to the representative of the operator of the network or other persons authorised to carry out network protection duties if the information is necessary to carry out those duties.[6]

Importantly, the Bill limits disclosure of information for disciplinary purposes to Commonwealth agencies, security authorities, or eligible State authorities.[7] Whereas the exposure draft would have allowed all network operators, including consumer internet Service Providers (ISPs) to collect and disclose intercepted communications for disciplinary purposes, the Bill provides adequate security to the privacy of private individuals. The Bill allows disclosure by the representative of the operator of the network to an appropriate law enforcement agency if the information is reasonably suspected to be relevant to determining whether another person has committed a prescribed offence.[8]

Finally, the Bill introduces a requirement to destroy records of intercepted communications as soon as practicable after they are determined not to be required.[9] This requirement appears to apply to all persons to whom the intercepted communications can lawfully be communicated, apart from law enforcement agencies.

The Bill, in its current form, satisfactorily and reasonably addresses the concerns EFA raised about the exposure draft. EFA believes that the Bill provides an appropriately limited exception for permissible interception of telecommunications for network security purposes. EFA assumes that the interests of the particularly government agencies in overseeing their networks are appropriately considered by the altered provisions of the Bill. EFA welcomes the changes that limit interception and disclosure of communications for ensuring that networks are 'appropriately used' to government agencies.

Minor issues in the new Bill

While EFA supports the Bill in its current form, we note that there are several areas in which it could be further amended to provide additional clarity.

The meaning of 'destroy'

Proposed s 79A provides that a record of an intercepted communication must be destroyed as soon as practicable after it is determined that it is not likely to be required for network security purposes or disciplinary action. It is not clear, however, what the requirements are for the destruction of such records. For example, 'destroy', in this situation, could mean merely 'delete', where the data remains

5 Telecommunications (Interception and Access) Amendment Bill 2009 (Cth), Schedule 1, cl 11.

6 Telecommunications (Interception and Access) Amendment Bill 2009 (Cth), Schedule 1, cl 15 (proposed s 63C).

7 Telecommunications (Interception and Access) Amendment Bill 2009 (Cth), Schedule 1, cl 15 (proposed s 63D).

8 Telecommunications (Interception and Access) Amendment Bill 2009 (Cth), Schedule 1, cl 15 (proposed s 63E). 'Prescribed offence' is defined in s 5 of the *Telecommunications (Interception and Access) Act 1979* (Cth) as:

(a) a serious offence, or an offence that was a serious offence when the offence was committed;
(b) an offence against subsection 7(1) or section 63; or
(ba) an offence against subsection 108(1) or section 133; or
(c) an offence against a provision of Part 10.6 of the Criminal Code ; or
(d) any other offence punishable by imprisonment for life or for a period, or maximum period, of at least 3 years; or
(e) an ancillary offence relating to an offence of a kind referred to in paragraph (a), (b), (c) or (d) of this definition.

9 Telecommunications (Interception and Access) Amendment Bill 2009 (Cth), Schedule 1, cl 22.

on the storage media but the index providing its location is removed. Records 'deleted' in this way remain accessible to those who have access to the physical media. Alternatively, 'destroy' could be read to require more secure forms of removal of the records. EFA submits that the requirement to destroy intercepted communications should explicitly reference acceptable standards of secure electronic document destruction as appropriate to the sensitive nature of intercepted communications.

The enumeration of persons required to destroy records

Proposed s 79A provides that a record of an intercepted communication must be destroyed if it is in the possession of a limited number of persons – a responsible person for the network, the individual or body who operates the network, or a person engaged in network protection duties in relation to the network. It appears that this list exhaustively lists the persons to whom intercepted communications may be lawfully disclosed under the Bill, excluding law enforcement agencies. EFA notes, however, that there will be no positive obligation to destroy communications that are unlawfully communicated to other parties not explicitly named in s 79A(1)(b). EFA submits that a new (iv) be inserted into s 79A(1)(b) to include all other persons who are aware or have notice that the communication was intercepted for network security purposes and that a duty to destroy exists. EFA acknowledges that law enforcement agencies and others who may have a legitimate interest in retaining such records may need to be explicitly excluded from such a broadened provision.

The lack of an obligation to destroy records no longer required

The requirement to destroy records under proposed s 79A only applies "as soon as practicable after [a relevant person becomes] satisfied that the restricted record is not likely to be required" for network protection duties or for disciplinary action purposes.[10] The prospective nature of this phrasing suggests that there is no requirement to destroy a record of an intercepted communication once the legitimate purpose for which it was intercepted has been fulfilled. EFA submits that proposed s 79A(2) be amended to additionally require destruction of applicable records as soon as practicable after the relevant person becomes satisfied that the record is no longer likely to be required.

The lack of protection for voice messages in electronic form

Proposed paragraph 7(3) provides that the power to intercept does not apply to voice communications in the form of speech. The Explanatory Memorandum (**EM**) explains that data relating to VoIP speech "may be interrogated but the data cannot be reconstructed in order to listen to the actual voice communication. "[11] The EM continue to explain that:

> This limitation is intended to preserve the integrity of the interception warrant regime by excluding telephone conversations and communications from the exception so that normal voice communications cannot be listened to.
>
> The limitation does not prevent recorded voice communications embedded in video or audio files such as music videos or audio files downloaded from the internet that may be attached to an email communication from being intercepted, reconstituted and listened to for the purposes of communicating or making use of communications intercepted under new paragraph 7(2)(aaa).[12]

It is not clear why the prohibition on assembling voice data should apply only to some voice communication and not to recorded voice communications embedded in video or audio files. It

10 Telecommunications (Interception and Access) Amendment Bill 2009 (Cth), Schedule 1, cl 22.

11 Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2009 (Cth), 9.

12 Explanatory Memorandum, Telecommunications (Interception and Access) Amendment Bill 2009 (Cth), 9.

appears that this latter category may extend to such communications as voice mail messages transmitted as audio files by email, which is an increasingly common practice. It is not apparent why any video or audio files intercepted ought to be allowed to be reconstituted and listened to or watched for network protection purposes (excluding any determination of whether a government network is being 'appropriately used'). EFA is unaware of network security purposes that would require reconstituting and listening or watching audiovisual content. Presumably, determining whether content contains dangerous material (for example, a virus or trojan) can be determined by automated examination of the data without the need to reconstitute and listen to or watch the recorded material.

EFA suggests that in the absence of a good reason why network security purposes should require audiovisual communications to be reconstructed, the prohibition on reconstructing Voice communications should be extended to all audiovisual communications.