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

Friday 07 August 2009

Telecommunications and Surveillance Law Branch
National Security Law and Policy Division
Attorney-General's Department
3-5 National Circuit
Barton ACT 2600

By email to: tslb@ag.gov.au

TIAA Amendments: Computer Network Protection

The Attorney-General's Department has called for submissions to the exposure draft on the computer network protection amendments to the *Telecommunications (Interception and Access) Act 1979* (the TIAA) by 07 August 2009.

Electronic Frontiers Australia (EFA) welcomes the opportunity to submit comments to the exposure draft. 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.

Electronic Frontiers Australia Inc. (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.

Our major objectives are to protect and promote the civil liberties of users and operators of computer based communications systems such as the Internet, to advocate the amendment of laws and regulations in Australia and elsewhere (both current and proposed) that restrict free speech 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 would like to express its disappointment in the short time period allowed for comments on the TIAA amendments. It is our opinion that this review should have been started earlier, in sufficient time to allow a more thorough analysis and discussion of the proposed amendments.

Generally, EFA supports the Department's position "that communications should remain private except in clear circumstances where the law provides specific direction." Whilst we acknowledge that some exceptions to a general prohibition on interception are warranted for security-related purposes, EFA believes that the current exposure draft does not provide sufficient clarity or adequate protections for the privacy of network users.

'Appropriately used': s 6AAA, s 5(1), 63C

As currently expressed, the exposure draft allows a very broad discretion to network operators to intercept communications in order to monitor compliance with any applicable Acceptable Use Policies (AUPs). There is no legislative guidance as to what provisions will be deemed 'reasonable' within the meaning of s 6AAA(b).

Section 5(1) effectively provides that 'network protection duties' includes monitoring the content of communications in order to ascertain whether the network is 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 uses 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.

A common example can be found in AUPs that prohibit the use of peer-to-peer filesharing networks for the purposes of copyright infringement. In order to determine whether "the network is appropriately used", a network operator would be required to intercept all peer-to-peer traffic and attempt a determination of whether any given traffic streams are being used to communicate copyright material without the licence of the copyright owner. Not only is such a task difficult or impossible due to the inherent complexity of copyright law and need to analyse the scope of any potential licences or fair dealing defences, it seriously imposes on the privacy of network users who are using legitimate file-sharing protocols for non-infringing activity.

Another example may be an AUP that prohibits use of network resources for 'excessive personal use'. In order to build evidence of excessive use, the proposed amendments would allow a network operator to monitor the contents of all communications that appeared to be non-work related. It is unclear why the collection of the *contents* of such communications must be intercepted, rather than merely noting their existence. Under the proposed legislation, the contents of all personal emails, banking transactions, and other non-work related communications could be stored and disclosed for 'disciplinary purposes' under such a common AUP clause.

EFA is also particularly concerned as the contents of typically dense acceptable use policies are only rarely read and understood by internet users. Often, users may not be aware that their

private communications are potentially open to ongoing surveillance to ensure compliance with such documents.

EFA opposes the construction of 'appropriately used' in s 6AAA of the exposure draft. We submit that the definition in s 6AAA ought to be amended to reflect that operators are only entitled to intercept and monitor communications where those communications pose a threat to the security of the network itself. EFA notes that there are already laws in place which deal with the disclose of sensitive information, and that there are already civil and criminal procedures available to determine the origins and contents of communications that appear to contravene such laws. The proposed amendments have the dangerous effect of reversing the burden of proof for such monitoring, allowing network operators to monitor for compliance, rather than to seek disclosure once a prima facie case or reasonable suspicion of unlawful activity exists. To the extent that operators of networks require the ability to monitor the activities of their users, there is no justification for allowing substantive examination of the contents of communication as opposed to the envelope information - numbers and types of packets and their destinations.

'Disciplinary purposes': s 63C(3)

The meaning of 'disciplinary purposes' is not defined in the exposure draft. The operation of s 63C(3) provides a broad ability for network operators to disclose the substance of intercepted communications to an unlimited group of people for an undefined purpose. 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. In the two examples given above, the entirety of a network user's browsing history, filesharing traffic, personal emails, banking and e-commerce transactions are available to be disclosed to any other person who is in a position to 'determin[e] whether disciplinary action should be taken' in relation to the user's network use.

These provisions radically alter the existing law and presumptions of privacy in network communications. EFA are not aware of any pressing reasons to allow such broad disclosure in monitoring compliance with AUPs. EFA submits that network owners are already in a sufficiently empowered position to restrain violations of AUPs - by blocking network services and classes of websites - without the need to actively monitor the substance of communications of network users. EFA submits that s 63C(3) ought to be omitted from the draft legislation.

Alternatively, if s 63C(3) is to remain in the proposed legislation, EFA submits that it ought to be amended to require that disclosure is only permitted to certain specifically named persons or organisation roles, and only for certain specifically provided purposes within the appropriate

written agreement. EFA submits that such certainty is a minimum requirement for a reasonable expectation of privacy in network use. Without such a limitation, users may find that their sensitive communications are disclosed to any of a large range of potential persons who may have an interest in the broad topic of 'disciplinary purposes' - including persons external to the organisation.

EFA is also greatly concerned about the potential for abuse of such exceptions by law enforcement agencies. By making a request to a network operator, a law enforcement officer would be able to rely on a broad prohibition on 'illegal behaviour' that is typically found in AUPs in order to justify interception and disclosure of communications without an interceptions warrant. This is likely to result in significantly less judicial oversight of law enforcement agencies, and appears not to have been contemplated in the issues paper. EFA submits that the proposed legislation be clearly amended to prevent disclosure to law enforcement agencies or other persons not concerned with security testing.

Disclosure for network protection purposes: s 63C(1)

The exposure draft does not limit the recipient of intercepted information for network protection purposes. EFA believes that recipients of such information ought to be limited to those who are authorised by the network operator and have a legitimate interest in receiving the communications for network protection purposes only.

EFA submits that s 63C(1) should be strengthened to require that communications of intercepted information for network protection purposes may only be made to another person who has been authorised in writing by the same Responsible Person who authorized the primary interception, and only if the disclosure is reasonably required by both persons in order to carry out their “network protection duties.”

Expectations of privacy of external network users

EFA is seriously concerned about the application of the proposed amendments to individuals who have not consented to the potential capture or disclosure of their communications with internal network users. The issues paper justifies certain interceptions on the basis that the individual concerned has, in all likelihood, agreed to an AUP that provides for interception, use, and disclosure of private communications. Even to the extent that this is a legitimate basis to allow interception, the exposure draft allows network operators to intercept communications addressed to internal users by external individuals who have never agreed to any such provisions.

For example, the exposure draft would allow the interception of private email communication

sent from an individual outside of the organisation to another individual within the organisation for the broad purposes of ascertaining the second individual's compliance with an Acceptable Use Policy.

EFA argues that there is no suitable justification to allow the interception and use of communications that originate from outside an organisation's network. EFA submits that the proposed legislation be amended to clearly require that only outgoing communications are open to interception for the purposes of network protection. Alternatively, if it is absolutely necessary for responses to requests that originate from within the organisation to be captured, EFA submits that only communication streams that originate from within the organisation ought to be open to interception, and that the proposed legislation ought to specifically exclude the interception of other incoming communications.

Application to consumer Internet Service Providers

The issues paper outlines an argument that corporate network operators require an ability to monitor the activity of employees on their networks. Even if this dubious conclusion is correct, the issues paper provides absolutely no justification for extending such interception exceptions to consumer internet service providers (ISPs). The draft legislation, however, makes no distinction between wholly private corporate networks and consumer ISP networks.

EFA argues that there is no evidence that consumer ISPs need an increased ability to monitor the activities of users for adherence to AUPs. Such a provision would have a greatly detrimental effect on consumer privacy, and should certainly not be introduced without greater justification and public debate. EFA notes that ISPs have not generally expressed a desire to be permitted to intercept household communications in order to monitor compliance, and further notes that such a provision is unlikely to increase public benefit to any extent that remotely approaches the harm to privacy interests of individual internet users.

EFA submits that the draft legislation should be amended so that it clearly operates only to the extent that it concerns communications by employees of organisations that provide network resources to employees in the course of their business.

EFA notes that the current exposure draft represents a radical shift in the ability, and potentially the duty, of ISPs to monitor communications between private individual subscribers. Such a shift is likely to be particularly relevant to the responsibility of ISPs to police private copyright infringement actions. Under the legislative safe harbour scheme in the *Copyright Act 1968* (Cth) s 116AH(2), an ISP is not required "to monitor its service or to seek facts to indicate infringing activity" and is in fact prohibited from doing so by the operation of the TIAA. The proposed changes would remove that prohibition, and radically alter the legislative balance

created by the introduction of the safe harbours by turning the previously prohibitory monitoring clause into a permissive clause.

EFA notes that the scope of the safe harbours is currently under judicial consideration by the Federal Court of Australia, and that the Minister for Broadband, Communications, and the Digital Economy has recently stated, in response to the Digital Agenda Review, that the legislative copyright balance will be monitored in the future.

EFA strongly argues that this is not an appropriate time to alter the responsibility or the ability of ISPs to intercept or monitor communications by their customers. EFA further argues that the pressing nature of this proposed legislation does not extend to a broad ability to monitor compliance with acceptable use policies, and such a provision should not be hastily enacted into Australian law. Accordingly, EFA reinforces its submission that this legislation be amended such that it does not alter the prohibition on consumer ISPs to intercept, monitor, or disclose communications from or to their subscribers.