Australian Government
Attorney-General's Department

National Security
Law and Policy Division

Telecommunications (Interception and Access) Amendment Bill 2009

Submissions provided to the Committee contain a number of suggestions aimed at enhancing aspects of the Telecommunications (Interception and Access) Amendment Bill 2009 (the Bill). The following additional information is provided to assist the Committee's consideration of these submissions.

1.1 Additional guidance regarding proposed network protection provisions

The Office of the Privacy Commission suggests that additional guidance on the operation of the provisions to assist organisations to train authorised persons in relation to what actions are lawfully permitted to be taken under the scheme.

The provisions allow an owner of a computer network to undertake necessary actions to operate, protect and maintain that network. The provisions are not compulsory and not defined because the types of activities undertaken may vary for each network across the private and public sphere, requiring different types of protection, operation and maintenance activities to be undertaken in differing circumstances.

The Explanatory Memorandum provides a useful source of guidance and gives some examples of who might be the 'responsible person' in an organisation, who can undertake network protection duties, and in what sort of circumstances information can be communicated.

The Attorney-General's Department is also available to provide guidance and advice regarding the operation of the network protection provisions in the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) and will undertake targeted education if the proposals are passed.

1.2 Secondary use or disclosure

A number of submissions raised concerns with the secondary use and disclosure of information access under the proposed provisions in the Bill.

The amendments contained in this Bill limit secondary use and disclosure of information obtained through network protection duties to:

a. network protection duties (as defined by the Bill)

b. undertaking disciplinary action against an employee of specified government agencies, office holder or contractor who has been given access to a network, and

c. reporting illegal behaviour that attracts a minimum of three years imprisonment penalty threshold to the relevant authorities.

A person undertaking network protection duties may use or disclose to another person where the use or disclosure is required for that person to perform network protection duties. This takes into account the fact that more than one person may be engaged to undertake network protection duties and will need access to the information in order to effectively perform their functions.

Additionally, the provisions provide for the use and disclosure of information accessed for network protection purposes as the responsible person may have to make a decision regarding ongoing network protection duties or consider whether information should be referred to a law enforcement agency if he or she reasonably suspects that the information is relevant to determining whether someone has committed certain criminal offences. This protects user privacy by ensuring that a network owner should only pass on information to a law enforcement agency about serious matters.

Only designated government security authorities and law enforcement agencies can specifically undertake network protection activities for the purpose of monitoring appropriate use of the network by employees. This exception reflects the sensitive nature of work undertaken by employees in these particular organisations and the additional professional standards and statutory requirements that are not applicable to other public sector or non-government organisations.

Network protection activities for disciplinary purposes will be limited to the conditions set out in a written user agreement, provided those conditions are reasonable. A person who receives lawfully intercepted information obtained through network protection activities, and anyone they pass it on to, cannot use or disclose the information for disciplinary purposes if to do so would contravene another Commonwealth, State or Territory law.

The proposed amendments to section 73 also restrict the further use and disclosure of this information to the purpose for which it was originally disclosed.

It is important to note that the other use and disclosure prohibitions contained in Part 2-6 of the TIA Act also apply to information obtained through network protection activities, restricting the further use of this information.

1.3 Disciplinary action

The Office of the Privacy Commission has suggested that the provisions in the Bill relating to disciplinary action should be limited to disciplinary action regarding the misuse of the computer network that pose a risk to network security only.

The provisions in the Bill allow specified government organisations the ability to access information to determine ‘appropriate use’ of the network by employees. The information accessed may then be used and disclosed for disciplinary purposes where appropriate. The specified government organisations include law enforcement, national security, defence and international relations organisations.

This exception reflects the current position whereby these organisations are able to monitor all communications passing over their computer networks for the purpose of protecting their network or for the enforcement of professional standards, but provides additional privacy protections by limiting the secondary use and disclosure of information and requiring reasonable terms and conditions of access to the network.

As stated above, this position reflects the sensitive nature of work undertaken by employees in these particular organisations and the additional professional standards and statutory requirements that are not applicable to other public sector or non-government organisations.

It is important to note that information accessed from a computer networks server is fully accessible to the network operator and is outside the operation of the Interception Act. Therefore limiting the use of information obtained under the proposed 'appropriate use' provisions to disciplinary proceedings, as requested by the Australian Federal Police association, would not be of any benefit.

1.4 Application of IPPs and NPPs

The Office of the Privacy Commission has raised concerns regarding the application of IPP's 10 and 11 and NPP 6.

Clause 15 is intended to preserve the operation of any relevant legislation in federal, state or territory law and therefore the amendments do not change the application of the IPPs to Commonwealth agencies.

Information intercepted by a person performing network protection duties is likely to be screened and copied only where it is necessary to perform those particular functions. In the majority of cases it is likely that these functions will be undertaken electronically and will only be viewed and retained in circumstances that require further investigation or action to be taken and the information must be destroyed when they are no longer required for that purpose. It is not considered necessary to provide individuals with access to personal information contained in intercepted communications in these circumstances.

1.5 ***Destruction of original records and copies***

A number of submissions have raised concerns regarding the destruction of communications accessed under the proposed provisions.

The Bill provides that original records of a communication that are obtained for the purpose of network protection duties security must be destroyed when no longer needed for that purpose. The ordinary meaning of the word 'destroy', to ruin, spoil, render useless, do away with or extinguish, would apply. This is considered appropriate as the appropriate destruction method will depend on the individual technologies and telecommunications networks used by the specific organisation.

Once the responsible person is satisfied that the original record is not likely to be required for a person to perform their network protection duties, the responsible person must cause the original record to be destroyed. This is the same in the case of a Commonwealth agency, security authority or eligible authority of a State. However, the responsible person in these

designated organisations must also be satisfied that the restricted record is not likely to be required in relation to any disciplinary action regarding use of the network.

The destruction requirements for information obtained through network protection activities are consistent with the destruction requirements for all lawfully intercepted information which stems from recommendations of the Telecommunications Interception Policy Review undertaken by Mr Peter Ford in May 1999 and implemented in the *Telecommunications (Interception) Legislation Amendment Act 2000*. The rationale being that provisions imposing an obligation to destroy a copy that may be outside the control of an individual or an organisation was unenforceable.

1.6 Voluntary disclosure of communications

The Law council of Australia is concerned that the Bill does not expressly prohibit or prevent an agency from requesting the disclosure of information accessed under the proposed provisions.

The context around which the provisions in Chapter 4 of the TIA Act, which the Law council is referring to (sections 174 and 175) are substantially different to Part 2-6 of the TIA Act where the proposed provisions will sit. In the case of the former, the prohibition against disclosure sits in the *Telecommunications Act 1997* and the exceptions to disclosure are located in the TIA Act.

This is different to part Part 2-6 of the TIA Act, where section 63 includes the general prohibition against disclosure of intercepted warrant information and the subsequent sections then provide exceptions to this. As such, it is not considered that explicit prohibitions are required. Guidance has been provided in the Explanatory Memorandum by explaining that in the absence of an exception that expressly allows law enforcement agencies to obtain such network protection information, information cannot be obtained in this way.

1.7 Voice communications

Electronic Frontiers Australia has questioned the requirement for audiovisual communications to be reconstructed.

The limitation on intercepting speech when undertaking network protection activities is designed to protect the integrity of the interception regime by ensuring that normal voice communications cannot be intercepted without proper lawful authority. However, voice communications in the form of voice or sound files, such as MP3 files or podcasts, can be listened to as this type of communication is markedly different from a telephone conversation between two or more people.

It is important to note that audiovisual files pose a significant threat to security of networks in that they may contain hidden viruses or Trojans. While the files may be identified in their packet form as being of threat, the packets may need to be reconstructed and listened to in order to fully understand and prevent further similar threats.

1.8 Concluding remarks

The amendments will allow the owner or operator of a computer network, or a person authorised in writing to perform network protection duties, to undertake all legitimate activities relating to operating, maintaining and protecting their network. This is an important step forward which

matches the growth in sophisticated attacks with the capacity to defend a network at the earliest possible point.

The Bill ensures that network protection activities cannot be undertaken without reason nor can the information obtained through these activities be used for any purpose. Rather, the Bill maintains the integrity of the interception regime by balancing the need to protect networks from malicious attack with clear limitations on the circumstances in which the access, use and disclosure of information will be permitted.