The Senate

Legal and Constitutional Affairs Legislation Committee

Telecommunications (Interception and Access) Amendment Bill 2009 [Provisions]

November 2009

© Commonwealth of Australia
ISBN: 978-1-74229-203-8

This document was printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

MEMBERS OF THE COMMITTEE

Members

Senator Patricia Crossin, **Chair**, ALP, NT

Senator Guy Barnett, **Deputy Chair**, LP, TAS

Senator David Feeney, ALP, VIC

Senator Mary Jo Fisher, LP, SA

Senator Scott Ludlam, AG, WA

Senator Gavin Marshall, ALP, VIC

Secretariat

Mr Peter Hallahan	Secretary
Mr Greg Lake	Principal Research Officer
Ms Cassimah Mackay	Executive Assistant

Suite S1. 61	Telephone:	(02) 6277 3560
Parliament House	Fax:	(02) 6277 5794
CANBERRA ACT 2600	Email:	legcon.sen@aph.gov.au

TABLE OF CONTENTS

GLOSSARY OF TERMS

Throughout this report a number of technical terms are used. To help the reader, this glossary includes a simple definition of a selection of common terms.

Stored communication is defined in subsection 5(1) of the TIA Act. It means a communication that is held on equipment that is operated by a telecommunications carrier/network. For a communication to be a stored communication, it cannot be accessed by a person who is not a party to the communication without the assistance of an employee of the operator and must not be passing over a telecommunications system.

A communication is taken to be ***passing over*** a telecommunications system from when it is sent or transmitted by the person sending the communication until when it becomes accessible to the intended recipient of that communication.

Generally, the term ***communication*** is used generically and includes a message or conversation in the form of speech, music or other sounds, data, text, visual images (animated or otherwise) or any combination of the above.

A ***restricted record*** is defined in subsection 5(1) of the TIA Act. It means a record (other than a copy) that was obtained by means of an interception, whether lawful or not, of a communication passing over a telecommunications system.

RECOMMENDATIONS

Recommendation 1

3.42 The committee recommends that the Bill be passed.

Recommendation 2

3.43 The committee recommends that these amendments be reviewed five years after their commencement.

CHAPTER 1

INTRODUCTION

Purpose of the Bill

1.1 On 17 September 2009, the Senate referred the provisions of the Telecommunications (Interceptions and Access) Amendment Bill 2009 (the Bill) to the Legal and Constitutional Affairs Legislation Committee for inquiry and report by 26 October 2009. The Senate later agreed to extend the reporting date to 16 November 2009.

1.2 Among other things, the Bill amends the *Telecommunications (Interceptions and Access) Act 1979* (the TIA Act)[1] to ensure that all owners and operators of computer networks can undertake legitimate activities to operate, maintain and protect their networks. The bill will also enable Commonwealth agencies, security agencies and eligible State authorities to ensure that the computer network is appropriately used by employees, office holders or contractors of the agency or authority.

Background

1.3 In 2008, the temporary exemption that enabled the interception and security agencies, as well as certain Government departments, to access communications on their own computer networks for network protection activities was extended to 12 December 2009. This extension was intended to allow the exemption to operate on an interim basis while a comprehensive solution covering both the public and private sectors was developed.

Conduct of the Inquiry

1.4 The Committee advertised the inquiry in *The Australian* newspaper on 23 September 2009 and 7 October 2009 and invited submissions by 9 October 2009. Details of the inquiry, the Bill and associated documents were placed on the Committee's website. The Committee also wrote to 67 organisations and individuals notifying them of the inquiry.

1.5 The Committee received 7 submissions which are listed at Appendix 1. The Committee did not hold any public hearings.

Acknowledgements

1.6 The Committee thanks those organisations and individuals who made submissions and provided information to the inquiry.

---

1 The TIA Act was renamed from the *Telecommunications (Interceptions) Act 1979* in 2006.

Note on references

1.7 References in this report are to individual submissions as received by the Committee, not to a bound volume.

CHAPTER 2

OVERVIEW OF THE BILL

2.1 The primary objective of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) is to:

> …protect the privacy of individuals who use the Australian telecommunications system. The TIA Act makes it an offence to intercept communications or to access stored communications, other than in accordance with the provisions of the Act. The… TIA Act [also] specif[ies] the circumstances in which it is lawful to intercept, access communications or authorise the disclosure of telecommunications data.[1]

2.2 The Bill seeks to amend the TIA Act to ensure that network operators can undertake legitimate activities aimed at securing the integrity of their network and the information it contains.[2]

Legitimate network protection activities

2.3 In recent times, the use of online services by individuals, governments, businesses and the not-for-profit sector to store and transmit sensitive information has increased. Protecting information and computer infrastructure from disruption or malicious access by criminal elements seeking to gain a financial or other benefit is therefore a growing priority for governments and computer network owners.[3]

2.4 Network owners and operators typically use automated network protection systems to screen and reject incoming communications if it is suspected that they contain a virus and network operators are able to monitor internal and outbound communications (including emails and internet browsing) provided they have obtained the consent of people using the network.[4]

2.5 While the use of gateway control systems (such as virus protection software) does not generally violate interception legislation, network owners and operators

---

1 *Telecommunications (Interception and Access Act 1979*, Annual Report for the year ending 30 June 2008, p. 2.

2 The Hon Robert McClelland MP, Attorney-General, Second Reading Speech: Telecommunications (Interception and Access) Amendment Bill 2009, *House of Representatives Hansard*, 16 September 2009, p. 9708.

3 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 1.

4 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2008*, p. 3.

undertaking network protection activities at the threshold of a network are vulnerable to inadvertent technical breaches of the TIA Act.[5]

> Whether an activity is lawful depends on the particular characteristics of the activity that is undertaken, where it is undertaken, by whom, and whether or not there is awareness by the affected person that it is being done. For example, persons undertaking network protection activities may need to copy a communication before it is delivered to the intended recipient. However, under the TIA Act, copying is only allowed at certain points in the delivery of that communication and under certain conditions.[6]

2.6 The main interception prohibitions contained in the TIA Act are found in sections 7 and 108. These sections prohibit interception of telecommunications that are passing over a telecommunications system and access to stored communications, except in accordance with a telecommunications interception warrant.

2.7 The TIA Act also contains special exemptions for security agencies and certain Government departments to allow access to communications on their own computer networks for network protection activities and for the enforcement of professional standards. These 'network protection provisions,'[7] contained in section 5F(2) and 5G(2) of the TIA Act, have the effect of providing a temporary exemption from the section 7 requirements for certain employees with responsibility for network protection or maintenance and allow these government employees to access and/or copy any communication from within or passing over the agencies' network for the enforcement of professional integrity. As the Attorney-General's Department submission explained:

> These provisions were originally introduced by the *Telecommunications (Interception) Amendment Act 2006* in order to allow the Australian Federal Police (AFP) to protect its network and to ensure staff were complying with the AFP's professional standards. At the time, Parliament legislated a two year sunset period for the provisions in order to allow consideration of a more comprehensive solution.
>
> In 2007, the provisions were widened to the current form to allow government agencies and authorities with a security or law enforcement focus to monitor communications for the purpose of protecting their networks and enforcing professional standards without the risk of breaching the TIA Act.[8]

---

5 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2008*, p. 3.

6 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 1.

7 The Hon Robert McClelland MP, Attorney-General, Second Reading Speech: Telecommunications (Interception and Access) Amendment Bill 2008, *House of Representatives Hansard*, 20 February 2008, p. 836.

8 Attorney-General's Department, *Submission 3*, p. 2.

2.8 In May 2008 the committee reported on an inquiry into the *Telecommunications (Interception and Access) Amendment Act 2008*. The main purpose of that Bill was to extend sunset provisions that apply to the network protection provision to allow sufficient time for the development of a comprehensive solution covering both the public and private sectors.[9] At that time, the Committee recommended that:

> …if further legislation proposing amendments to the network protection provisions (including to sunset clauses) is introduced, such legislation should include a thorough and considered response to achieving a balance between individual privacy rights and network protection requirements. Such a review should assess mechanisms to mitigate intrusiveness and abuse of access, and consider how secondary data may be managed appropriately.[10]

2.9 According to the Explanatory Memorandum, this Bill amends the TIA Act:

> …to implement a full legislative solution that clarifies the basis on which communications can be accessed for the purposes of protecting a computer network.[11]

Existing Arrangements

2.10 As stated above, the primary objective of the TIA Act is to protect the privacy of individuals who use the Australian telecommunications system.[12] One way the TIA achieves this is by prohibiting the interception of a communication that is 'passing over' a telecommunications system.[13]

2.11 Existing section 5F defines when a communication is considered to be 'passing over' a telecommunications system. Broadly, a communication is taken to start passing over a telecommunication system when it is sent or transmitted by the sending person – paragraph 5F(1)(a) – and is taken to continue to pass over the system until it becomes accessible to the intended recipient – paragraph 5F(1)(b). For example, an email is taken to start passing over a telecommunications system when the email is sent and is taken to finish passing over that system when it becomes accessible to the intended recipient (i.e. it 'arrives' in the recipient's email inbox).

---

9 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 1.

10 Senate Standing Committee on Legal and Constitutional Affairs, *Report into the Telecommunications (Interception and Access) Amendment Bill 2008*, May 2008, p. 17.

11 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 1.

12 *Telecommunications (Interception and Access) Act 1979*, Annual Report for the year ending 30 June 2008, p. 2.

13 Subsection 7(1), *Telecommunications (Interception and Access) Act 1979.*

2.12 Existing subsection 5F(2) alters that definition by stating that, if the communication is sent from an address on a computer network operated by a Commonwealth agency, security agency or eligible authority of a state, it is not taken to have started passing over the telecommunication system until it is no longer under the control of certain employees (i.e. those responsible for managing the agency's network or those responsible for the enforcement of professional standards in the agency).

2.13 Defining when a communication is passing over a telecommunication system in this way has the effect of enabling:

> …communications which are within the network boundaries of the relevant agency or authority's network to be copied or recorded in order to allow *network protection duties* concerning the operation, protection or maintenance of the network, or upholding professional standards, to be performed by personnel within those bodies other than the sender.[14]

2.14 Existing section 5G similarly modifies the definition of the 'intended recipient' to allow certain communications within Commonwealth agencies, security authorities and eligible authorities of a State to be copied or recorded. Subsection 5G(2) outlines that such interception may only be conducted:

> …in order to allow duties concerning the operation, protection or maintenance of the network, or upholding professional standards, to be performed by personnel within those bodies other than the addressee.[15]

2.15 Both subsections 5F(2) and 5G(2) are the subject of sunset clauses (contained in subsections 5F(3) and 5G(3) respectively) meaning they cease to have effect at the end of 12 December 2009. After this date, employees of Commonwealth agencies, security authorities and eligible authorities of a State with network protection responsibilities would require a warrant to copy or record communications, even in the course of their network protection duties.

The Proposed Arrangements

2.16 The Bill seeks to establish a permanent regime that will:

- enable all owners and operators of computer networks to undertake activities to operate, maintain and protect their networks;
- enable Commonwealth agencies, security authorities and eligible State authorities to ensure that their computer network is appropriately used by employees, office holders or contractors of the agency or authority;

---

14 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 6.

15 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 6.

- limit secondary use and disclosure of information obtained through network protection activities to:
  - network protection purposes;
  - undertaking disciplinary action against an employee, office holder or contractor of a Commonwealth agency, security authority and eligible authority of a State who has been given access to a network; and
  - reporting illegal behaviour that attracts a minimum of three years' imprisonment penalty threshold to the relevant authorities; and
- require the destruction of records obtained by undertaking network protection activities when the information is no longer required for those purposes.

Interceptions for Network Protection Purposes

2.17 The Bill (at Items 5-8), by repealing subsections 5F(2), (3) and 5G(2), (3) and (4), seeks to simplify the definition of when a communication is passing over a telecommunication system (and the definition of 'intended recipient') so that the definition applies generically, regardless of whether the communication is sent from within a government agency or not.

2.18 Item 11 of the Bill then inserts paragraph 7(2)(aaa), which lifts the prohibition on the interception of a communication by a person (contained in subsection 7(1)) if the person is appropriately authorised to engage in network protection duties and it is necessary for the person to intercept the communication in order to perform those duties effectively.

2.19 Importantly, the proposed regime would allow certain authorised people in both government and non-government agencies to intercept non-voice communications for network protection purposes.[16] That is, the regime contained in the Bill would not be limited in application to employees of Commonwealth agencies, security authorities and eligible authorities of a State (though it would apply in these agencies). Furthermore, this exception would not be subject to a sunset clause.

2.20 Item 13 of the Bill inserts a paragraph which ensures that the prohibition contained in subsection 7(1) still applies to a voice communication in the form of speech (including a communication that involves a recorded or synthetic voice).

2.21 As the Explanatory Memorandum explains:

> In the case of Voice over Internet Protocol (VoIP), the voice communication in the form of packet data may be intercepted and

16 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 8.

> interrogated but the data may not be reconstructed in order to listen to the actual voice communication.
>
> 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.
>
> Recorded voice communications embedded in video or audio files such as a music video or audio file downloaded from the internet that may be attached to an email communication can be intercepted, reconstituted and listened to for the purposes of communicating or making use of communications intercepted under new paragraph 7(2)(aaa).[17]

'Appropriate use' of Government Networks

2.22 The Bill allows network owners and operators from both the private and public sectors to intercept communications in certain circumstances, particularly where that interception is necessary for network protection purposes. Only Government network operators, however, will be able to intercept communications to ensure that staff use the network appropriately.

2.23 Item 9 of the Bill inserts new section 6AAA. Section 6AAA defines when a network is 'appropriately used' by an employee, office holder or contractor of a Commonwealth agency, security agency or eligible authority of a State. An employee's use of the network is considered appropriate when they have undertaken (in writing) to use the network in accordance with reasonable (written) conditions specified by the agency and where their use is in compliance with those conditions.

2.24 This definition of 'appropriate use' is designed to be flexible enough to recognise that what constitutes appropriate use of a computer network may vary between agencies.[18]

2.25 While user agreements must be reasonable and must comply with all relevant Commonwealth, State and Territory laws,

> …[t]he Bill does not require a new user agreement to be entered into. Existing user agreements will suffice where an employee, office holder or contractor of an agency or authority has undertaken to comply with the conditions set out in the agreement and those conditions are reasonable.[19]

---

17 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 10.

18 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 7.

19 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 7.

2.26 Furthermore, the absence of an agreement does not preclude an agency or authority from recording information transiting their network for duties relating to the operation, protection or maintenance of the network.

> However, an agency or authority will not be able to record information transiting their network to ensure the network is appropriately used, nor secondarily use or disclose information accessed for disciplinary purposes. This is because new subsection 63D(2) at Item 15 only authorises disciplinary action to be taken in relation to 'appropriate use' of the network, not 'use' of the network.[20]

Secondary use and disclosure

2.27 The Bill also limits the use and disclosure of information obtained through network protection activities to activities relating to the protection of the network, the reporting of illegal behaviour (where that behaviour attracts a minimum penalty of three years' imprisonment) to the relevant authority, and to undertaking disciplinary action against an employee, office holder or contractor of a Commonwealth agency, security authority and eligible authority of a State who has been given access to a network.

Network Protection

2.28 Item 15 of the Bill also inserts new sections 63C which sets out the terms under which a person engaged in network protection duties may communicate or make use of the information they intercept.

2.29 Subsection 63C(1) and (2) allow a person engaged in network protection duties to disclose that information which has been lawfully intercepted in the course of their duties or to disclose that information to another person with network protection duties if it is reasonably necessary to enable the other person to perform their duties. These subsections are limited by new subsection 63C(3) which does not allow the use or disclosure of a communication that has been converted into a voice communication in the form of speech.

2.30 Items 17-20 of the Bill:

> …ensure that the limitations on the use and disclosure of information related to disciplinary action will apply to further use and disclosures regardless of the number of times the information is used or disclosed. These amendments will also ensure that a person who receives information related to disciplinary action under subsection 63D(2), may only communicate, use or record that information where doing so does not contravene another law of the Commonwealth or a State or Territory.[21]

---

20 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 7.

21 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, pp. 12-13.

Disciplinary purposes

2.31 Item 15 of the Bill inserts new section 63D, allowing a person engaged in network protection duties to disclose (lawfully) intercepted information to another person in order to determine whether disciplinary action should be taken. This provision limits this on-disclosure to determinations about the appropriate use of a network by an employee who is an employee or office holder (or contractor) of a Commonwealth agency, security authority or eligible State authority and who has legitimate access to that network.[22]

Destruction of records

2.32 A 'restricted record' is defined in subsection 5(1) of the TIA Act as 'a record other than a copy that was obtained by means of an interception, whether or not in contravention of subsection 7(1), of a communication passing over a telecommunications system.'[23]

2.33 Current section 79 of the TIA Act sets out that where a 'restricted record is not likely to be required for a permitted purpose in relation to the agency, the chief officer must cause the restricted record to be destroyed. These requirements only currently apply to interception agencies. As stated in the Explanatory Memorandum, the new provisions:

> …when combined with the new destruction requirements under new section 79A at Item 22 would create a different regime for interception agencies. [Requiring the same regime] would impose an onerous administrative burden on agencies as the destruction requirements in section 79 are imposed on an agency's chief officer. In practice this would mean that the chief officer of an agency would need to destroy every record of a network protection activity when it is no longer needed. In some agencies this could amount to thousands of records at any point in time.[24]

2.34 The Bill seeks to address this by inserting new subsection 79(3) which ensures that new section 79A will apply to any records intercepted for network protection duties (under new paragraph 7(2)(aaa)) while section 79 would only apply to interception agencies.

2.35 Records of a communication intercepted under proposed paragraph 7(2)(aaa) must be destroyed once the responsible person (that is, the individual or head of the body which operates the network) is satisfied that the record is not likely to be required for network protection duties.

---

22 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 11.

23 *Telecommunications (Interceptions and Access) Act 1979*, subsection 5(1), definition of 'restricted record'.

24 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 13.

2.36 Where the network is operated by a Commonwealth agency, security authority or eligible authority of a State and the communication was intercepted for the purpose of determining whether disciplinary action should be taken (or taking that action), the responsible person must cause that record to be destroyed as soon as practicable after becoming satisfied that the record is not likely to be required.[25]

Definition of 'permitted purpose'

2.37 Schedule 2 of the Bill contains a number of provisions which amend or supplement the definition of 'permitted purpose'. Many of these amendments clarify current practices or alter the definition to reflect changes in other acts.

2.38 Item 2 inserts new subparagraph 5(1)(b)(v), which clarifies that lawfully intercepted information can be communicated in seeking or issuing a control order pursuant to Division 104 of the *Criminal Code*. Currently, section 67 of the TIA Act allows lawfully intercepted information to be used for a 'permitted purpose', which includes a purpose connected with an investigation by the AFP of a prescribed offence (defined). This amendment clarifies the TIA Act to avoid doubt that the AFP may use and communicate lawfully intercepted information when seeking the Attorney-General's approval, to apply for an interim control order, or when applying for the control order to the courts. New subparagraph (b)(vi), which is also inserted by this item, clarifies that lawfully intercepted information can also be used or communicated in relation to preventative detention orders sought and issued pursuant to Division 105 of the *Criminal Code*.[26]

2.39 According to the Explanatory Memorandum:

> The amendments to *permitted purpose* in relation to the use or disclosure of information related to Divisions 104 and 105 of the *Criminal Code* are designed to clarify the operation of the existing legislation, rather than expanding police powers.[27]

2.40 Item 14, contained in Part 2 of Schedule 2 of the Bill is designed to ensure that AFP officers who have, in good faith, used or communicated lawfully intercepted information for a purpose connected with Divisions 104 and 105 of the *Criminal Code*, are not liable for any breach of the TIA Act caused by that use or communication.[28]

---

25 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 13.

26 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, pp. 15-16.

27 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 24.

28 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 24.

2.41 Items 3 and 4 of Schedule 2 amend the 'permitted purpose' definition to reflect changes to the *Police Integrity Commission Act 1996* (NSW). This includes amendments to facilitate the transfer of particular functions from the Independent Commission Against Corruption to the Police Integrity Commission. The amendments also ensure that further changes to that Act will be recognised by the TIA Act without the need for further amendments to the Commonwealth Act.[29]

Delegation powers for certificate etc

2.42 Section 18 of the TIA Act currently contains an evidentiary certificate regime for intercepted and stored communications. The regime allows the Managing Director or secretary of a carrier (or of a subsidiary of a parent company of a carrier) to issue a written, signed certificate setting out such facts as he or she considers relevant with respect to acts or things done by, or in relation to, employees of the carrier. These certificates set out facts in relation to a warrant issued to the Australian Security and Intelligence Organisation (ASIO) and include facts that may be relevant in order to have a warrant issued or executed as well as relevant facts pertaining to anything done by an employee of the organisation in connection with the execution of the warrant. These certificates may be received in evidence in exempt proceedings (defined) without further proof and are conclusive evidence of the matters stated in the certificate.

2.43 Items 9-12 of Schedule 2 of the Bill retain this power but allow the Managing Director or secretary to delegate their evidentiary certificate functions by authorising, in writing, an employee of the carrier to issue such a certificate. Although this provision will expand the number of people who can issue evidentiary certificates under section 18 on behalf of a carrier:

> …[e]nabling staff who are more accessible but of sufficient seniority to issue the certificate gives the carrier flexibility, which should ensure that evidentiary certificates can be issued promptly.[30]

2.44 As the Explanatory Memorandum explains:

> …[t]he delegation of this function is consistent with the current evidentiary certificate regime applying to law enforcement interception warrants under section 61 of the TIA Act.[31]

2.45 Item 11 of Schedule 2 makes a similar amendment to section 129, allowing a similar delegation in relation to written evidentiary certificates relating to acts or

---

29 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 16.

30 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 18.

31 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 18.

things done to enable the execution of a stored communications warrant (as opposed to a warrant issued to ASIO).

Telecommunications data to be included in evidentiary certificates regime

2.46 Telecommunications data is information about a communication, other than the content or substance of the communication itself. For example, for a telephone-based communication, telecommunications data would include subscriber information, the telephone numbers of the parties involved, the time of the call and its duration. In relation to internet-based applications, it would include the Internet Protocol (IP) address used for a session and the start and finish time of each session.[32]

2.47 Telecommunications data is available in relation to all forms of communications, including fixed and mobile telephony services and internet based applications, including internet browsing and Voice over Internet Protocol (VoIP).[33]

2.48 Under the current regime, telecommunications data may only be disclosed by a carrier to ASIO in connection with the performance of its functions and to enforcement agencies for the investigation of criminal law, a law imposing a pecuniary penalty or the protection of the public revenue.[34]

2.49 Item 13 of Schedule 2 of the Bill inserts three new sections, 185A, 185B and 185C, which extends the evidentiary certificate regime (discussed above, but also including certificates issued by the Director-General or the Deputy Director-General of Security) to include access to telecommunications data obtained under an authorisation. The new sections apply to historical and prospective telecommunications data and are consistent with the existing evidentiary certificate provisions for interception and stored communications.

---

32 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 20.

33 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 20.

34 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 20.

CHAPTER 3

KEY ISSUES

3.1 The Committee received 7 submissions to the inquiry which canvassed a number of different issues. While there were very few issues that were raised by more than one submitter, generally the concerns related to either how intercepted information could be used or the adequacy of the destruction requirements for records of intercepted communications.

Use of intercepted information

3.2 The proposed exemptions from the prohibition on intercepting communications that are passing over a telecommunications network apply differently to different types of organisations. Broadly, both government and non-government owners and operators of computer networks will be able to intercept communications for 'network protection duties'. However, only certain government agencies will be allowed to use intercepted communications for 'disciplinary action'. Various submitters raised concerns about how well these two terms were defined. The majority of other issues raised during the inquiry relate when information that has been intercepted must or may be disclosed.

'Network Protection Duties'

3.3 Generally, the proposed arrangements would allow authorised persons within any organisation that owns or operates a network to intercept communications for 'network protection duties'. The Office of the Privacy Commissioner (OPC) called for a more precise explanation for what constitutes 'network protection duties':

> The [OPC] suggests that the legislation could provide additional guidance on the operation of the provisions to assist organisations to train authorised persons about what actions are lawfully permitted to be undertaken under the scheme (including clause 11). For example, what measures are covered by 'the operation, protection or maintenance of the network' and when is an interception 'reasonably necessary'?[1]

3.4 The Attorney-General's Department (AGD) indicated that the provisions, which do not require organisations to undertake network protection duties, do not define the specific actions necessary to operate, protect and maintain a network as the types of activities required may vary for each network across the private and public sphere.

---

1 Office of the Privacy Commissioner, *Submission 2*, p. 4.

> 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… and will undertake targeted education if the proposals are passed.[2]

3.5 Another submitter, who practices law and advises on information technology matters, also called for clarification as to what sorts of activities would constitute 'reasonable use'. The submitter cited common and desirable industry practices such as spam filtering, employee absence arrangements such as email redirections, and common email quarantining practices as examples which may not strictly be considered necessary for the protection of the network but which should be considered lawful.[3]

'Disciplinary Action'

3.6 The OPC pointed out that 'disciplinary action' is not defined in the bill and noted that new section 6AAA sets out that the parameters used to determine appropriate use of the computer network would be based on the Commonwealth agency, security authority or eligible State authority's IT policies.

> The Office notes that IT policies often include conditions that are not related to computer network protection, although these conditions may be reasonable in the circumstances. For example, an IT policy may regulate individuals' use of the computer network for non-work related purposes, such as internet banking.[4]

3.7 The OPC is concerned that the broad scope of the 'appropriate use' definition may make it lawful for the agency to use and disclose an intercepted communication for disciplinary action even if that use of the network does not pose a network security risk. The OPC recommended that the Bill should clarify that 'disciplinary action' regarding misuse of the computer network applies only to those activities that pose a risk to network security.[5]

3.8 The AGD submitted that the broader application of the provisions was appropriate in that they:

> …[reflect] the sensitive nature of work undertaken by employees in these particular organisations and the additional professional standards and

---

2 Attorney-General's Department, *Supplementary Submission*, p. 2.

3 Name withheld, *Submission 1*, pp. 2-3ff

4 Office of the Privacy Commissioner, *Submission 2*, p. 4.

5 Office of the Privacy Commissioner, *Submission 2*, p. 5.

> statutory requirements that are not applicable to other public sector or non-government organisations.[6]

3.9 The Australian Federal Police Association (AFPA) further expanded on this issue, pointing out that, since the *Law Enforcement (AFP Professional Standards and Related Measures) Act 2006* repealed the disciplinary tribunal under s56 of the *Complaints (Australian Federal Police) Act 2981*, there has been no legislated internal appeal mechanism for non-reviewable matters (except in relation to termination under the *Fair Work Act 2009*). That is, the 'disciplinary action' definition contained in the Bill facilitates the use of intercepted communications for taking internal administrative or managerial action for low-level matters.

> The net result for AFP employees would be that the dealing of such information for disciplinary purposes, if used in an investigation under Part V of the *Australian Federal Police Act 1979*, may lead to a non-reviewable outcome with a punitive action. This unfairly impacts on those employed under the AFP Act compared with Commonwealth public sector employees, who are able to seek merit review as well as judicial review of disciplinary action taken using this evidence.[7]

3.10 The AFPA recommends that section 63D be amended to use the term 'disciplinary proceedings' (instead of 'disciplinary action') to provide express exclusion of low-level, internal administrative and managerial actions. This would ensure that section 63D would only relate to cases where an independent body will have the power to hear or examine the evidence presented under oath.

3.11 The AGD responded to this recommendation, saying:

> 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.[8]

Law Enforcement

3.12 Item 14 in Part 2 of Schedule 2 includes a provision which validates the communication, use or recording of certain information, including that which has occurred prior to the commencement of the Bill. The Attorney-General's Department (AGD) submission explained the inclusion of this retrospective provision.

> The Criminal Code contains provisions that enable the AFP to apply for control or preventative detention orders in order to prevent a terrorist attack…

---

6 Attorney-General's Department, *Supplementary Submission*, p. 3.

7 Australian Federal Police Association, *Submission 5*, p. 4.

8 Attorney-General's Department, *Supplementary Submission*, p. 4.

> The [AGD] is of the view that the nature of the offences associated with control orders and preventative detention orders means that the AFP is authorised to use lawfully intercepted information in these applications. However, the issue has not been considered by a court and, in the absence of a specific reference, there is some risk a court could find that information obtained under the TIA Act is not available for these purposes. [9]

3.13 The AGD submitted that this provision will remove any uncertainty and ensure the validity of information used in control order applications. Furthermore, they submitted that the amendments preserve the status quo and do not increase the powers and functions of law enforcement agencies under the TIA Act. [10]

Disclosure

3.14 The TIA Act makes disclosure of lawfully intercepted information to another person an offence unless that disclosure is an exempt disclosure. Broadly, disclosure that may be relevant in determining whether a serious offence has been committed is considered an 'exempt disclosure'. The Law Council of Australia raised concerns that the proposed disclosure provisions could allow law enforcement agencies to bypass existing warrant arrangements. The OPC suggested that the secondary use and disclosure provisions should be strengthened.

Voluntary Disclosure to Law Enforcement Agencies

3.15 The Law Council of Australia raised concerns about proposed section 63E which allows the voluntary disclosure of information that has been intercepted for network protection purposes to enforcement agencies. While agreeing to the principle of the provision, they were concerned that this may allow law enforcement agencies to obtain information by request, thus bypassing the warrant arrangements contained elsewhere in the TIA Act.

> The Law Council accepts that an agency would not have the power under the Act to compel the disclosure of such information. However, the Law Council submits that an agency is not expressly prohibited or prevented from requesting the disclosure of information under proposed section 63E.
>
> Chapter Four [of the TIA Act] also contains voluntary disclosure provisions… which are similar in effect to proposed section 63E. These provisions permit information to be disclosed in the absence of a formal authorisation where it is necessary for certain purposes, such as the enforcement of the criminal law. Unlike proposed section 63E, the voluntary disclosure provisions in Chapter Four expressly provide that the section does not apply where ASIO or the enforcement agency has requested the disclosure of the information. In that way, the voluntary

9 Attorney-General's Department, *Submission 3*, p. 5.

10 Attorney-General's Department, *Submission 3*, p. 6.

> disclosure provisions in Chapter Four can not be used to circumvent the authorisation process.[11]

3.16 The Law Council submitted that section 63E should contain a similar arrangement to the Chapter Four disclosure laws, restricting the disclosure of information where an enforcement agency has requested that information. They maintained that such an amendment would safeguard against the potential misuse of the section to circumvent the warrant requirements in the TIA Act.[12]

3.17 The AGD has addressed this concern in their supplementary submission.

> The context around which the provisions in Chapter 4 of the TIA Act… 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.[13]

Secondary Use and Disclosure

3.18 In its submission to the inquiry, the OPC noted that the responsible person for a network is permitted to further disclose lawfully intercepted information if that person suspects, on reasonable grounds, that the information may be relevant in determining whether a prescribed offence (usually an offence that is punishable by a prison term of a maximum of at least three years) has been committed.[14] The OPC considered that any exceptions that allow the further disclosure of restricted records should be well defined.

> These exceptions should align with community expectations and be based on clearly articulated public policy reasons.[15]

3.19 The OPC also raised concerns about the strength of the disclosure provisions in relation to non-government agencies.

---

11 Law Council of Australia, *Submission 4*, p. 2.

12 Law Council of Australia, *Submission 4*, p. 2.

13 Attorney-General's Department, *Supplementary Submission*, p. 5.

14 Office of the Privacy Commissioner, *Submission 2*, pp. 4-5.

15 Office of the Privacy Commissioner, *Submission 2*, p. 5.

> Except for a designated Commonwealth agency, a security authority or eligible authority of a state, there appears to be no restrictions on any secondary uses or disclosures of the intercepted information placed on: (a) a person engaged in network protection duties, or (b) on the responsible person, or (c) on their employer. The Office suggests that s.63C could be strengthened to prohibit secondary uses or disclosures by such persons and their employer.[16]

3.20 The AGD believe that the broader protections contained in the TIA Act relating to the use and disclosure of information are sufficiently strong.

> 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.[17]

Other comments on disclosure

3.21 Electronic Frontiers Australia (EFA) noted the changes made to the bill since the Exposure Draft released by the Attorney-General's Department on 17 July 2009.[18] EFA were less concerned about agency misuse of the provisions.

> Importantly, the Bill limits disclosure of information for disciplinary purposes to Commonwealth agencies, security authorities, or eligible State authorities.
>
> 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.[19]

Destruction Requirements

3.22 Section 79 of the TIA Act requires an interception agency to destroy 'restricted records' (which does not include a copy of that record) if the Chief Officer of the agency is satisfied that the restricted record is not likely to be required for a permitted purpose. Evidence received by the Committee related to the destruction of original records (and when the destruction requirement should apply), and whether or not the destruction requirements should apply to copies of the original record.

---

16 Office of the Privacy Commissioner, *Submission 2*, pp. 4-5.

17 Attorney-General's Department, *Supplementary Submission*, p. 3.

18 A copy of the discussion paper and exposure draft is available at: *http://www.ag.gov.au/www/agd/agd.nsf/Page/Consultationsreformsandreviews_Telecommunications(InterceptionandAccess)AmendmentBill2009-NetworkProtection* (accessed 14 October 2009)

19 Electronic Frontiers Australia, *Correspondence*, p. 3.

Original records

3.23 The Bill contains an exemption for communications that were intercepted for computer network protection within interception agencies. As explained by the OPC:

> Clause 21 to the Bill states that the requirements of s.79 do not apply to a communication that was intercepted for computer network protection by an interception agency. The EM states that this obligation would pose an onerous administrative burden on such agencies as the responsibility is placed on the chief officer of the agency rather than on an authorised officer (such as a 'responsible officer').
>
> Accordingly, a new provision (s.79A) is introduced relating to the destruction of a restricted record as soon as practicable if it is not likely to be required for specified purposes. The provision applies generally to computer network protection (including interception agencies) and the obligation to destroy the restricted record is placed on the 'responsible officer'.[20]

3.24 The OPC submitted that all intercepted records, including copies, obtained for the purpose of network protection should be destroyed when no longer needed for that purpose.[21]

3.25 The EFA also commented on the new provisions relating to the destruction of records. They note that the requirement only applies 'as soon as is practicable after the responsible person becomes satisfied that the restricted record is not likely to be required'.

> 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.[22]

3.26 The EFA argued that proposed section 79A(2) should be amended to require the destruction of applicable records as soon as practicable after the relevant person becomes satisfied that the record is no longer likely to be required. Although the distinction appears slight, the EFA argued that it was important that this more explicit requirement be included.[23]

3.27 The AGD explained the position taken by the Bill:

> 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

---

20 Office of the Privacy Commissioner, *Submission 2*, pp. 6-7.

21 Office of the Privacy Commissioner, *Submission 2*, pp. 6-7.

22 Electronic Frontiers Australia, *Correspondence*, p. 4.

23 Electronic Frontiers Australia, *Correspondence*, p. 4.

> 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.[24]

Copies of records

3.28 New section 79A of the TIA extends only to the destruction of the original record of a communication intercepted under 7(2)(aaa). The Explanatory Memorandum states that:

> There is no obligation on the *responsible person* to destroy copies of restricted records as often they are no longer in the possession of the *responsible person*, but have been lawfully communicated to another person.[25]

3.29 The Australian Law Reform Commission (ALRC) noted that:

> Section 150 of the TIA contains a similar requirement to destroy information or a record obtained by accessing a stored communication. However, this section does not distinguish between a record and a copy of a record.[26]

3.30 In his report into the regulation of access to communications in August 2005, Anthony S Blunn AO said that:

> The Interception Act definition of restricted record is curious in excluding a copy of a record even though the definition of 'record' includes a copy. Thus it would appear possible for agencies to avoid what appears to be to be the clear intent of the Act simply by copying the 'record'.[27]

3.31 The ALRC recently conducted an inquiry into Privacy in Australia. This inquiry culminated in the production of the report entitled 'For Your Information: Australian Privacy Law in Practice', which was tabled in Parliament on 11 August 2009.[28] During that inquiry:

> A number of stakeholders… expressed the view that the same destruction rules should apply to records and copies of records.[29]

3.32 In their submission to this inquiry, the ALRC pointed out that:

---

24 Attorney-General's Department, *Supplementary Submission*, p. 4.

25 Explanatory Memorandum, *Telecommunications (Interception and Access) Amendment Bill 2009*, p. 14.

26 Australian Law Reform Commission, *Submission 6*, p. 2.

27 Mr Anthony A Blunn AO, *Report of the Review of the Regulation of Access to Communications*, August 2005, p. 69.

28 Australian Law Reform Commission, *Submission 6*, p. 1.

29 Australian Law Reform Commission, *Submission 6*, p. 3.

> [According to the AGD]… the requirement to destroy copies was excluded from s 79 because of enforcement issues. For example, agencies could not enforce destruction of copies given to other agencies for permitted purposes, or where the information appeared on the public record. The AGD also noted that copies of lawfully intercepted information may be made only in limited circumstances under the TIA, and that any copies of the information continued to be protected from further use or communication.[30]

3.33 The ARLC submitted that, if copies of information obtained from a stored communication warrant must be destroyed, the same destruction requirements should apply to copies of information obtained from an interception warrant. The recommended that the 'Data Security' principle under the Unified Privacy Principles, which provides that an agency or organisation must destroy or render non-identifiable personal information if it is no longer needed, should apply to records as well as copies of intercepted information.[31]

3.34 The AGD, in their supplementary submission, further emphasised the rationale behind excluding a destruction requirement for copies, saying that imposing such an obligation may be outside the control of an individual or an organisation and was therefore unenforceable.[32]

Other Issues

3.35 The OPC also raised two issues not covered by any other submitters dealing with the importance of allowing individuals to access intercepted information relating to them and the need for a review of the amendments.

Accessing intercepted communications

3.36 The OPC submitted that the Bill should include a provision modelled on National Privacy Principle (NPP) 6.1 which allows an affected person to access intercepted information relating to them. They argued that an essential component of an effective privacy framework is the ability of anyone to access their own personal information. The inclusion of an access provision may assist in achieving an appropriate balance between the competing public interest in maintaining computer network protection and individual privacy.[33]

3.37 The AGD argued that it was not necessary to provide individuals with access to personal information contained in intercepted communications.

---

30 Australian Law Reform Commission, *Submission 6*, p. 3.

31 Australian Law Reform Commission, *Submission 6*, p. 3.

32 Attorney-General's Department, *Supplementary Submission*, p. 4.

33 Office of the Privacy Commissioner, *Submission 2*, p. 6.

> 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.[34]

Review of the act

3.38 The OPC recommended that the operation of these amendments should be independently reviewed five years after their commencement.[35]

Conclusions

3.39 Generally, submitters did not feel that the Bill was clear about what types of behaviour would be considered necessary for 'network protection duties' and what constituted 'disciplinary action'. Some submitters felt that the proposed disclosure regime for information that had been lawfully intercepted could be strengthened. They submitted that this would prevent law enforcement agencies from circumventing warrant arrangements and ensure that the provisions were in line with community expectations. There was also some concern about the absence of a requirement to destroy copies of restricted and that the destruction requirement for original records was not strong enough.

3.40 However, submitters who gave evidence to the Committee were generally supportive of the principles of the Bill. There was agreement that network owners and operators should be allowed to protect the security of their networks. Furthermore, it was deemed to be appropriate that only Commonwealth agencies, security authorities and eligible State authorities should be allowed to intercept communications for certain disciplinary purposes.

Committee View

3.41 The Committee feels that the concerns raised by submitters have been satisfactorily addressed by the AGD in its supplementary submission. As such, the Committee feels that the Bill should be passed. The Committee also notes the 2008 recommendation that the any permanent network protection mechanism be reviewed to ensure that it mitigates against intrusiveness and abuse of access, and considers how secondary data may be managed appropriately.[36] The Committee still feels that a review of the amendment contained in this Bill is desirable.

---

34 Attorney-General's Department, *Supplementary Submission*, p. 4.

35 Office of the Privacy Commissioner, *Submission 2*, p. 7.

36 See Senate Standing Committee on Legal and Constitutional Affairs, *Report into the Telecommunications (Interception and Access) Amendment Bill 2008*, May 2008, p. 17.

Recommendation 1

3.42 The committee recommends that the Bill be passed.

Recommendation 2

3.43 The committee recommends that these amendments be reviewed five years after their commencement.

Senator Trish Crossin
Chair

ADDITIONAL COMMENTS BY LIBERAL SENATORS

1.1 In order to be effective, legislation designed to ensure that network owners and operators are able to protect their networks must be clear. In particular, the law must provide clarity as to what types of actions network owners and operators, including those operating networks for government agencies, can lawfully undertake.

1.2 Liberal Senators are concerned that the Bill does not provide sufficient clarity as to what actions would be considered necessary to effectively undertake 'network protection duties' and, further, how intercepted information may be used for 'disciplinary purposes'.

1.3 The Law Council of Australia ('the Law Council') also raised some important concerns about proposed section 63E and the potential for law enforcement agencies to bypass warrant arrangements to obtain information using voluntary disclosure provisions.

'Network Protection Duties'

1.4 Proposed paragraph 7(2)(aaa) provides an exemption from the prohibition on intercepting communication if the person is authorised to engage in network protection duties and the interception is necessary for the performance of those duties. Neither the Bill nor any supporting material provide sufficient examples for what types of actions constitute 'appropriate use' of the network for 'network protection duties'. A number of submitters to the inquiry raised this concern.

1.5 One submitter recognised that some network administrators may unwittingly engage in unlawful behaviour because of this lack of clarity.

> Some of these are everyday activities that almost all network administrators would do and users would accept without thinking there is any possibility of contravening the TIA Act.[1]

1.6 The Office of the Privacy Commissioner suggested that additional guidance be provided to help organisations train authorised persons about what actions are lawfully enabled under the proposed exemption.[2] While the Explanatory Memorandum provides examples of people who might be considered appropriate to undertake network protection duties, no guidance is given as to what actions they might then appropriately take.

---

1 Name withheld, *Submission 1*, p. 2.

2 Office of the Privacy Commissioner, *Submission* 2, p. 4.

'Disciplinary Action'

1.7 The Office of the Privacy Commission noted that 'disciplinary action', in relation to the misuse of computer networks within designated Commonwealth Agencies, security agencies and eligible authorities of a state, was not defined. Some IT policies include provisions that are unrelated to network protection.

1.8 Liberal Senators are concerned that, unless the government clarifies that 'disciplinary action' only applies to activities that pose a risk to network security, network owners or operators could use and disclose an intercepted communication for disciplinary action even though that use of the network does not pose a network security risk.

Recommendation 1

1.9 That the Government provide greater clarity about what activities do and don't constitute 'network protection activities'.

1.10 That the Government make it clear that 'disciplinary action' only applies to activities that pose a risk to network security.

Voluntary Disclosure

1.11 Proposed section 63E of the Bill allows lawfully intercepted information to be voluntarily disclosed to certain agencies (including law enforcement agencies) by the person responsible for the network, if the person suspects that the information is relevant to determining whether another person has committed a prescribed offence. A 'prescribed offence' is generally an offence punishable by imprisonment for a maximum period of at least three years.

1.12 The Law Council supports the principles underpinning this provision but raised concerns that some law enforcement agencies may attempt to bypass existing warrant arrangements by requesting that information be 'voluntarily disclosed'. In their submission, the Law Council noted that it would be of great concern if:

> …law enforcement agencies were to use this voluntary disclosure provision to obtain information by request, when they would otherwise require a warrant to access it…
>
> …The Law Council accepts that an agency would not have the power under the Act to compel the disclosure of such information. However, the Law Council submits that an agency is not expressly prohibited or prevented from requesting the disclosure of information under proposed section 63E.[3]

3 Law Council of Australia, *Submission* 4, p. 2.

1.13 Liberal Senators support the Law Council's proposal that the Bill be amended to provide that proposed section 63E does not apply where an agency has requested the disclosure of the information. The Law Council submitted that:

> …such an amendment would safeguard against the potential misuse of the section to circumvent the warrant requirements of the Act.[4]

Recommendation 2

1.14 That proposed section 63E of the Bill should be amended to provide that the section does not apply where an agency has requested the disclosure of the information.

Senator Guy Barnett **Senator Mary Jo Fisher**

Deputy Chair

4 Law Council of Australia, *Submission* 4, p. 2.

DISSENTING REPORT BY AUSTRALIAN GREENS

1.1 Unfortunately the Committee was unable to hold a hearing into this Bill which makes yet another set of amendments to the Telecommunications Interception Act, in this case to allow interception, copying, recording and disclosure of electronic communications in the name of protecting computer networks from malicious access and building confidence in the online world. It also allows specified government organisations – law enforcement, national security, defence and international relations - to intercept communications and undertake disciplinary actions ensure that computer networks are appropriately used.

1.2 While much improved through consultation on an August exposure draft, during the Inquiry into this Bill the Privacy Commissioner, Electronic Frontiers Australia and the Australian Law Reform Commission recommended minor amendments to a) clarify definitions of what constitutes "network protection duties" and "disciplinary actions" b) tighten requirements to destroy copies of intercepted communications.

1.3 The Australian Greens concur that these amendments are necessary to clarify the Bill and strengthen its safeguards and are not satisfied that the Attorney General's Department adequately addressed these suggestions when dismissing them.

1.4 The Attorney General claims that network protection activities vary for each network and therefore cannot be defined, however, given that this is the pretext for this suite of amendments it is not inappropriate that parameters should be set and the scope and nature of activities more clearly defined. The Privacy Commissioner asked, "what measures are covered by 'the operation, protection or maintenance of the network' and when is an interception 'reasonably necessary?'

1.5 The Attorney states that imposing an obligation to destroy copies of lawfully intercepted information is unenforceable. As the Australian Law Reform Commission submitted, arising from the Commission's thorough inquiry into privacy issues, there is, "no reason why copies of information obtained from a stored communication warrant must be destroyed but copies of information obtained from an interception warrant are not… The covert nature of interception and access to communications requires the safeguard that the intercepted or accessed information is destroyed as soon as it is no longer required."

1.6 Given these issues were thoughtfully raised, and could easily be addressed through minor amendments, the Australian Greens do not share the Committee's view that the Bill should be passed without amendment.

Senator Scott Ludlam

APPENDIX 1

SUBMISSIONS RECEIVED

Submission Number	Submitter
1.	Name Withheld
2.	Office of the Privacy Commissioner
3.	Attorney-General's Department
4.	Law Council of Australia
5.	Australian Federal Police Association
6.	Australian Law Reform Commission
7.	WA Police, Office of the Deputy Commissioner

ADDITIONAL INFORMATION RECEIVED

1 Correspondence regarding inquiry - provided by Electronic Frontiers Australia on Friday 9 October 2009

2 Correspondence provided to assist the committee in consideration of submissions received - provided Sunday 8 November 2009

APPENDIX 2

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

The committee did not hold any public hearings in relation to this inquiry.