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