CHAPTER 3

EXTENSION OF NETWORK PROTECTION SUNSET DATES

3.1 Several submissions commented on the proposed extension of the sunset clauses for network protection exemptions. When these provisions were first introduced to Parliament in the Telecommunications (Interception) Amendment Bill 2006, the Minister stated that network protection was an issue for both public and private organisations and that a policy proposal to allow appropriate, lawful access for network administrators was the subject of ongoing consultation. Since then these provisions have been amended only to allow additional law enforcement agencies, not corporate agencies, to be exempt under the provisions.

3.2 The Law Council of Australia (Law Council) submission noted that sunset clauses are included in legislation for a number of purposes, including to:

- ensure that certain legislative provisions only remain in operation as long as is necessary to address a temporary emergency situation;
- compel the periodic review of the operation of a controversial provision; and
- provide a temporary measure to respond to a particular problem, while a more permanent solution is developed.[1]

The Law Council noted that the sunset clauses relating to network protection fulfil the third purpose.

3.3 In submissions to the inquiry, the Australian Privacy Foundation and the Law Council proposed that consideration of a further extension of the sunset clauses relating to network protection should be based on further information. In particular, these parties contended that the Senate should be provided with information on progress toward a more permanent solution, particularly for corporate entities, on why such a solution is not in place, and whether and why a further eighteen months is required.

3.4 Addressing the issue of progress towards a longer-term solution, the Attorney-General's Department submitted that:

> While significant progress has been made by the Department towards a full legislative solution, the additional 18 months will allow adequate time to finalise the policy development and undertake consultation with state and territory governments and a broad range of non-government stakeholders.

---

1 *Submission* 1, p. 14.

> The additional 18 months will also allow for any issues raised during these consultations to be fully considered and incorporated where appropriate.[2]

3.5 When asked by the committee about the extent of progress to develop a long term solution, the Attorney-General's Department responded:

> We have been developing a discussion paper which has not gone outside the Attorney-General's Department. What has become clear, as we look into the problem, is that technology is moving very quickly. The types of threats to critical infrastructure are changing every single day and so we are looking at the scope of any possible solution to address the kinds of challenges that we are dealing with. We work with our critical infrastructure protection area in the department very closely and it is with them that we are actually looking at the scope of any solution.[3]

3.6 In relation to why the Department needed a further 18 months for the process, representatives said that:

> …essentially we are taking into that time the fact that we have just had an election so that slowed down any development of a particular policy. Now we want to ensure that we develop a solution that allows us to consult very broadly because there are a lot of stakeholders who will be affected by any change in legislation. We want to ensure that we do not need a further extension of time, so that is why we have sought 18 months.[4]

3.7 The committee also sought information from government representatives on whether corporate agencies may be in technical breach of the TIA Act in their current practices for virus scanning and email quarantine systems. A representative of the Attorney-General's Department acknowledged that this is a grey area, stating:

> The nature of computer networks is so different and complex that I could not comment on whether particular areas of industry or banking or whatever would be in technical breach of the act. What I can say is that when it is appropriate we constantly provide guidance to organisations when they ring up and talk about their filtering systems. You will find that a lot of organisations actually straightaway block emails of a particular attachment type because they know that they are likely to have problems embedded, even though they might be quite innocent. They also run electronic scanning, which is not in breach of the legislation. But we have identified that this is an area that is grey and that needs to be dealt with as quickly as we can. Certainly I am not aware of any organisation that is in technical breach of the legislation. As I have said, we welcome people to approach the department and seek guidance on how they can actually act and not be in breach of the legislation and still protect their networks.[5]

---

2 *Submission* 4, p. 2.

3 *Committee Hansard*, 17 April 2008, p. 28.

4 *Committee Hansard*, 17 April 2008, p. 28.

5 *Committee Hansard*, 17 April 2008, p. 35.

3.8 The committee also sought to clarify with other witnesses whether they had any specific concerns with the amendments relating to extension of the sunset dates contained in the Bill. A number[6] supported the submission of the Office of the Privacy Commissioner (OPC), which stated that:

> The Office supports the position of the Blunn Review that network protection provisions should be accompanied by appropriate privacy protections. Further, in the view of the Office, the subsequent widening of the scope of the network protection exemption to over 20 agencies makes it more important that the safeguards recommended by the Blunn Review are built-into the legislation, including for the purposes of the proposed 18 month extension to the sunset provisions.[7]

3.9 In relation to privacy protections, the OPC recommended that consideration be given to amending the Bill to contain the following more rigorous requirements:

(a) a prohibition on secondary use of any data accessed for the purpose of protecting the agency's network security, unless there are cogent public policy reasons which reflect community expectations;

(b) that agencies must clearly identify the people who are given the authorisation under exemptions; and

(c) that any data obtained for the purpose of network security should be immediately destroyed when it is no longer needed for that purpose.[8]

3.10 The committee notes that recommendation (b) is consistent with findings in the Blunn report. Both the OPC and the Blunn report also proposed a higher level of personal privacy protection for network protection provisions than is currently enshrined in the TIA Act. However, while their issues and recommendations are not mutually exclusive, the Blunn report raises additional issues in regards to voice data and evidence discovered in relation to criminal behaviour:

> There should be clear authorisation and the persons with that authority should be clearly identified. Those persons should be required to protect the privacy of any data accessed in the same way that the employees of C/CSPs [Carriage and Carriage Service Providers] are required to protect data accessed in the course of their employment. The vexed question is what should happen where such access discloses evidence of criminal behaviour. … In my view in both situations the content of the communication should be protected but the person with access may report their view that there may be evidence of criminality etc. The data, presumably other than voice data, could then be accessed as if it were a stored communication i.e. by search warrant. The question of the use of the content of voice data raises

6 Submissions 1, 8, 10.

7 Office of the Privacy Commissioner, *Submission* 7, p. 5.

8 Office of the Privacy Commissioner, *Submission* 7, pp 4-6.

significant evidentiary and other problems and should be separately considered.[9]

Committee findings and recommendations

3.11 The committee is aware of the rapidly changing nature of technology and of the sensitive nature of data held by security and law enforcement agencies. These agencies consequently face challenges in maintaining secure networks and professional standards—both of which the community expect them to maintain in a manner that safeguards rights, privacy and safety.

3.12 While developing 'technologically neutral' legislation may be difficult, almost eighteen months have passed since the sunset clauses were approved by Parliament. This timeframe was apparently established to allow the Attorney-General's Department to develop a full legislative solution to network protection issues for corporate entities and interception agencies.

3.13 Additionally, the Blunn report had proposed in 2005 that the network protection provisions should address both corporate and interception agency needs, and had raised a number of issues that needed to be resolved in terms of privacy and secondary data use. The issues raised by the Blunn report were not addressed in the Telecommunications (Interception) Amendment Bill 2006, partly due to its late insertion into the parliamentary program, and were also not addressed when additional agencies were given network protection exemptions in 2007.[10]

3.14 The committee considers that the recommendations made in the submission to this inquiry by the Office of the Privacy Commissioner in relation to privacy issues warrant further consideration, along with the unresolved issues raised in the Blunn report.

3.15 Since the Blunn report, the committee has now been asked on three occasions to consider the network protection issue, with little or no information being provided on the impacts on privacy and agency accountability. Furthermore, the so-called 'grey area' of monitoring and interception of data in corporate networks does not appear to have progressed beyond a draft policy within the Attorney-General's Department.

3.16 The committee considers that any future legislative amendment of the network protection provisions (including sunset clauses) 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.

---

9 A. S. Blunn, AO, *Report of the Review of the Regulation of Access to Communications*, 2005, p. 59.

10 These measures were contained in the *Telecommunications (Interception and Access) Amendment Act 2007.*

3.17 However, the committee considers that these issues can not be adequately addressed by amending the Bill, given the imminent expiry of the sunset clauses. Further, implementing a single change to ensure that the person to which the exemption applies is clearly identified would be an incomplete solution, which might reduce the likelihood of this issue being resolved in a more comprehensive way.

Recommendation 1

3.18 The committee recommends 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.