CHAPTER 5

OTHER AMENDMENTS

5.1 This chapter considers the remaining provisions of the Bill:

- The removal of the distinction between Class 1 and Class 2 offences.
- The removal of the TIRAC function.
- Items in Schedule 6.

Class 1 and 2 offences

5.2 Until now the interception regime has authorised interception on the basis of classes of offences. In the past only Class 2 offences required the issuing authority to have regard to privacy considerations. The offence distinctions have been removed and the offences are now termed 'serious offences'. Serious offences are defined in the new section 5D, and include murder or similar offences, kidnapping, offences under Division 307 of the Criminal Code (these include importation and possession of certain drugs and plants) terrorism offences, offences against Division 72, 101, 102 or 103 of the Criminal Code (terrorism offences); or an offence in relation to which the ACC is conducting a special investigation.

5.3 In his report, Mr Blunn explored the necessity for the classification of offences for the purposes of obtaining TI warrants. He found that law enforcement agencies found the classification 'over prescriptive' and occasionally a barrier to accessing data rather than a support.

5.4 The report continues:

> Given that the objective in the case of both Class 1 and Class 2 offences is to justify the issuing of an interception warrant and having regard to the similarity of the offences it is not clear why the distinction is made. Any significance can only be in terms of the processes relating to the issue of a warrant. The only difference between those processes is that in relation to Class 2 offences the issuing authority is required to have regard to the gravity of the offence and the extent of the interference to privacy involved. In the case of Class 1 the gravity of the offences is inherent and presumably is regarded as over-riding any privacy considerations.[1]

5.5 He concluded that the provision produces no meaningful difference in outcome, and adds to the length and complexity of an already convoluted Act. He recommended that 'those offences currently described as Class 1 and Class 2 offences be identified solely by reference to the prescribed term of imprisonment'.[2]

---

1 Blunn, p. 55.

2 Ibid.

5.6 The removal of the distinction was commented upon by the Law Council. The Council had serious reservations about much of the Bill, and considered that particularly in the case of B-Party intercepts, the existing Class 1 offences should be the only offences which allowed the issue of a warrant.[3]

5.7 Conversely, both the AFP[4] and Commissioner Hyde of the South Australian Police supported the proposal. Commissioner Hyde further suggested that:

> Another class of offence to capture corruption, child pornography and significant offending that does not carry a 7 year term of imprisonment should also be considered.[5]

5.8 The Explanatory Memorandum notes that the amendments are designed to 'simplify a complex area of the interception regime'. The Committee notes the Commissioner's suggestion, but considers that to add another class of offences at this point would defeat the purpose of simplification. Nevertheless, the offences he refers to are of sufficient seriousness that they may warrant consideration in any subsequent review of these provisions.

5.9 In general, the effect of the amendments is to bring privacy considerations to all warrant applications and not limit them to class 2 offences. The Committee welcomes this enhancement of the privacy protections available under the Act.

Removal of the TIRAC function

5.10 Schedule 5 of the Bill repeals the Telecommunications Interception Remote Authority Connection (TIRAC) function which is exercised by the AFP. The removal of this function from the AFP was a recommendation of the Blunn report.

5.11 TIRAC is described in the Explanatory Memorandum as

> … a historical electronic accountability mechanism which requires each interception agency to lodge its interception warrants with the AFP. The effect of this function is that the warrants do not take effect until the AFP receives the warrant and notifies the Managing Director of the carrier of the issue of the warrant.[6]

5.12 In his second reading speech, the Attorney General observed that:

> TIRAC's utility has been exhausted by technological developments, and the bill replaces the current requirements for AFP to facilitate warrants by a requirement for my department to scrutinise warrants immediately upon issue and maintain a register of warrants.

---

3 *Committee Hansard*, 15 March 2006, pp 2-3.

4 *Committee Hansard*, 15 March 2006, p. 32.

5 *Submission 16*, p. 3.

6 Blunn, p. .

> The act will continue to require all agencies to maintain comprehensive records as part of the interception regime which are subject to regular compliance inspections by the Commonwealth Ombudsman or equivalent state oversight body.[7]

5.13 This amendment, which is effectively an administrative one, was supported by the AFP, and was not a subject which elicited a great deal of comment by submitters or witnesses. The Committee considers that the change should be monitored to ensure that the effect of the amendments does not lower standards of efficiency or accountability.

Other amendments: Schedule 6

5.14 Schedule 6 of the Bill makes other amendments to the Act to ensure the ongoing effective operation of the interception regime in Australia.

5.15 The proposed amendments seek to:

- include an additional permitted purpose for use and communication of lawfully obtained information in relation to the Victorian Office of Police Integrity;
- clarify that employees of a carrier exercise authority under a telecommunications interception warrant when assisting law enforcement agencies in the execution of interception;
- remove the exception to the definition of interception in subsection 6(2) of the Act;
- update applicable reference to money laundering offences in New South Wales; and
- correct drafting errors within the Act which have been the result of previous amendments Acts.[8]

5.16 Generally, the amendments contained in Schedule 6 of the Bill have not been the subject of any objection throughout the inquiry.

5.17 One minor exception is the repeal of subsection 6(2).

5.18 Subsection 6(2) creates an exception to the general prohibition in subsection 7(1) against the interception of a communication in its passage of the Australian telecommunication system. At the commencement of the Act subsection 6(2) was intended to exempt the activities of telecommunications carriers and employees of the carrier from the general prohibition contained in subsection 7(1) to allow the testing of

---

7 *House of Representatives Hansard*, 16 February 2006, pp 9-10.

8 Explanatory Memorandum, p. 47.

the carrier's equipment to ensure that the network and associated equipment operated correctly.[9]

5.19 The Australian Bankers Association states that:

> Section 6(2) is consequently most useful in the context of emails where it is not possible to ensure that the person making the communications has 'knowledge' of any recording or listening activities. The repeal of the section may therefore impact on the ability of organisations to monitor incoming emails. This is a matter of grave concern in light of the need for organisations to perform, for various reasons, the routine interception and scanning of such communications.

5.20 However, the repeal of subsection 6(2) has been welcomed by many organisations. The Office of the Privacy Commissioner advised that:

> The Office supports the repeal of s. 6(2) of the Interception Act. This section has given rise to confusion in the past about the circumstances under which phone calls may be covertly monitored. The repeal of s. 6(2) will assist in reinforcing the privacy objects of the Interception Act.

5.21 Proposed section 108(2) sets out a number of exceptions to the general prohibition on access to stored communications. Subsection 108(2)(e) provides that the general prohibition does not apply in relation to:

> Accessing a stored communication by another person lawfully engaged in duties relating to the installation, connection or maintenance of equipment or a line, if it is reasonably necessary for the person to access the communication in order to perform those duties effectively

5.22 The Explanatory Memorandum states that:

> This exception provides that network or system administrators do not contravene the prohibition against interception by performing routine functions designed to prevent malicious content such as viruses from entering their networks.

Committee view

5.23 The Committee considers that the concern expressed that the repeal of subsection 6(2) impacts the ability to monitor incoming emails is addressed by the proposed exemptions to the general prohibition on stored communications in subsection 108(2).

5.24 The Committee also agrees with the view that the repeal of the subsection reinforces the privacy objectives of the Act.

---

9 Explanatory Memorandum, p. 48.

Recommendation 27

5.25 The Committee recommends that the amendments proposed in Schedule 6 of the Bill be passed.

Recommendation 28

5.26 Subject to the amendments set out above, the Committee recommends that the Bill be passed.

Senator Marise Payne
Committee Chair