CHAPTER 2

OVERVIEW OF THE BILL

Background

2.1 The purpose of the *Telecommunications (Interception) Amendment Bill 2006* (the bill) is to amend the *Telecommunications (Interception) Act 1979* (the Act) to implement certain recommendations of the *Report of the Review of the Regulation of Access to Communications* (the Blunn Report).

2.2 A major feature of the bill concerns lawful access to stored communications. There have been previous attempts to amend the Act to achieve this. They include provisions in the Telecommunications Interception Legislation Amendment Bill 2002 which proposed access to stored communications without the requirement for a telecommunications interception warrant. These provisions were withdrawn following a recommendation from the Committee that 'an interception warrant should be required for access to such communications.'[1]

2.3 Again, in February 2004, the Telecommunications (Interception) Amendment Bill 2004 provided that a telecommunications interception warrant would be required to obtain access to material which had not been retrieved by the intended recipient. A Committee inquiry found that that Bill was unclear about access to stored communications. The inquiry also revealed a disagreement between the Attorney-General's Department and the AFP as to the state of the existing legislation in relation to stored communications. The Committee recommended that Parliamentary consideration of the proposed subsections dealing with stored communications be deferred until the disagreement was resolved and Parliament was informed of the outcome.

2.4 A further amendment proposal in 2004, (the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004*) provided an interim access regime for stored communications pending the outcome of the Blunn Report. The amendments were to expire on 14 December 2005, but on 14 September 2005, were further extended until 14 June 2006, to allow time for the Government to fully consider the recommendations from the Blunn Report.

Overview of the Bill

Schedule 1: Stored communications

2.5 The stored communications amendments prohibit access to stored communications held by a telecommunications carrier, subject to certain limitations.

---

1 Bills Digest No. 111 2003-04

Access to stored communications

2.6 The bill introduces a warrant regime for enforcement agencies to retrieve stored communications held by a carrier. The amendments regulate the use, communication and recording of information obtained by access to stored communications and require the enforcement agencies to report to the Minister regarding the use of the stored communications powers.

Applications for warrant

2.7 Warrants are only available to an enforcement agency which is investigating an offence punishable by a maximum period of imprisonment of three years or a pecuniary penalty of at least 180 penalty units ($19,800).

2.8 The existing interception warrant applications are limited to law enforcement agencies such as the AFP and the Australian Crime Commission. However, the bill proposals also permit applications to be made by all agencies responsible for administering a law imposing a pecuniary penalty or administration of a law relating to the protection of the public revenue. This includes the Australian Customs Service, the Australian Tax Office, and the Australian Securities and Investments Commission. Similar State and Territory agencies are also included.

Issue of warrants

2.9 Warrants are issued by an issuing authority appointed by the Minister and may include Judges of Courts exercising Federal jurisdiction, a Federal Magistrate, or a magistrate. The appointment is contingent upon the nominated person accepting the appointment in writing. The Minister may also appoint Members of the AAT who are legal practitioners of at least 5 years' standing.

Definition of stored communications

2.10 The proposed definition of stored communication **(item 1)** provides that a stored communication is a communication that, among other things, is held on equipment operated by the carrier at its premises. The explanatory memorandum states that:

> This is to ensure that, …, the stored communications regime only applies to accessing stored communications via a telecommunications carrier. The regime does not affect existing lawful access to communications stored on a person's telecommunication device.

Use of information obtained under a stored communications warrant

2.11 The use or communication of information which is obtained from stored communications will be limited to matters connected with investigating an offence which is punishable by a maximum period of imprisonment of one year, or a pecuniary penalty of at least 60 penalty units.

Schedule 2: Access to communications from third parties

2.12 Schedule 2 provisions enable agencies to obtain an interception warrant for communications of an associate of a person of interest. These have been called the 'B Party' interception warrants.

Application for and issue of warrants

2.13 The warrant may only be issued where the investigation involves serious offences that attract a maximum penalty of seven years imprisonment. The provision also requires the issuing authority to be satisfied that:

- there are reasonable grounds for suspecting that a particular person is using, or is likely to use, the telecommunications service;
- information that would be obtained by interception would be likely to assist in connection with the investigation by the agency of the seven-year offence in which the suspect is involved; and
- the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the suspect.

2.14 When issuing the warrant, the issuing authority must also have regard to the following:

- the extent to which the proposed interception interferes with the privacy of any person;
- the gravity of the offences being investigated;
- the extent to which the information obtained under the warrant will assist the investigation;
- the extent to which alternative methods of investigation have been used or are available to the agency; and
- the extent to which these alternative methods would be useful to or would prejudice the investigation.

2.15 The warrant applications are accompanied by an affidavit, sworn by the representative of the applicant agency. These are provided for half the time of existing interception warrants – 45 days for law enforcement authorities and 3 months for ASIO warrants.

Schedule 3: interception of telecommunications services on the basis of a telecommunications device

2.16 The existing TI warrants are 'named person warrants'. These amendments are 'equipment-based' rather than attaching to the person who is recorded as the owner of the service. This will allow access to mobile phone text messages, as well as voice messages.

2.17 The issuing authority must only issue a warrant under this part unless satisfied that the applicant agency 'has no practicable methods of identifying the telecommunications services used or likely to be used by the person of interest, or that interception of those services would not be possible'.[2]

2.18 The Explanatory Memorandum to the bill notes that this covers instances in which agencies may be able to identify all services, but it is impracticable to intercept each service. The example given is the person who uses multiple SIM cards to evade interception.

Schedule 4: Removal of references to Class 1 and Class 2 offences

2.19 The interception regime has until now 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.

2.20 The privacy considerations now apply to all interception warrants.

Schedule 5: Transfer of functions

2.21 The Schedule changes the arrangements concerning the Telecommunications Interception Remote Authority Connection, an electronic system which requires the interception agency to lodge its interception warrants with the AFP. The Explanatory Memorandum to the bill indicates that the system has outlived its usefulness, and is to be discontinued.

2.22 The effect of this will be to allow warrants once issued to be executable immediately, rather than having to wait for them to be registered with the AFP. Registers will be kept by the Secretary of the Attorney General's Department who will receive and review warrants on issue.

Schedule 6

2.23 These provisions are largely consequential, and provide for specific state application where necessary. In addition, the use of interception powers by security and law enforcement agencies continues to be subject to strict reporting, disclosure and destruction provisions of the Act.

---

2 Explanatory Memorandum, p.34