

2004-2005-2006

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT BILL 2006

EXPLANATORY MEMORANDUM

(Circulated by authority of the Attorney-General,
the Honourable Philip Ruddock MP)

TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT BILL 2006

OUTLINE

1. The purpose of this Bill is to amend the *Telecommunications (Interception) Act 1979* to implement certain recommendations of the Blunn Report on the review of the regulation of access to communications under the *Telecommunications (Interception) Act 1979* (the Act).
2. The *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* introduced into the Act the concept of a 'stored communication' (paragraph 7(3A)) and provided that a stored communication could be intercepted without the need for a telecommunications interception warrant (paragraph 7(2)(ad)). Access to such communications could therefore be obtained by other lawful means, such as by a normal search warrant.
3. The stored communications amendments were intended as an interim measure pending a thorough consideration by Mr A S Blunn AO of how best to regulate access to communications in the ever-changing world of technologies. The amendments were originally subject to a 12-month sunset clause meaning that the provisions were to cease operation on 14 December 2005. The *Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005* extended the sunset date until 14 June 2006 to provide sufficient time to consider the recommendations of the Blunn Report. The Blunn Report was presented to Parliament on 14 September 2005 when the *Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005* was introduced.
4. In implementing recommendations of the Blunn Report, this Bill will amend the Act to:
 - (a) insert a warrant regime for access to stored communications held by a telecommunications carrier;
 - (b) enable interception of communications of a person known to communicate with the person of interest;
 - (c) enable interception of telecommunications services on the basis of the telecommunications device;
 - (d) remove the distinction between class 1 and class 2 offences for which telecommunications interception powers are available to law enforcement agencies; and
 - (e) remove the Telecommunications Interception Remote Authority Connection function currently exercised by the Australian Federal Police and transfer the associated warrant register function to the Department administering the legislation.
5. This Bill will also amend the Act to:
 - (a) remove the exception to the definition of interception in subsection 6(2) of the Act;

- (b) clarify that employees of a carrier exercise authority under a telecommunications interception warrant when assisting law enforcement agencies in the execution of interception;
- (c) include an additional permitted purpose for use and communication of lawfully obtained information in relation to the Victorian Office of Police Integrity; and
- (d) update applicable reference to money laundering offences in New South Wales.

FINANCIAL IMPACT STATEMENT

The amendments made by the Telecommunications (Interception) Amendment Bill 2006 will have no financial impact.

NOTES ON CLAUSES

Clause 1: Short title

The short title of this Act is the *Telecommunications (Interception) Amendment Act 2006*.

Clause 2: Commencement

This clause provides a table that identifies the day of commencement for the specified parts of the Bill.

Schedule 1 (Stored communications) will commence on the day on which this Bill receives Royal Assent.

Schedule 2 (B-party interception) will commence on the day after this Bill receives Royal Assent.

Schedule 3 (Equipment-based interception) will commence on the day after this Bill receives Royal Assent.

Schedule 4 (Class 1 and class 2 offences) commence on 1 July 2006.

Schedule 5 (Transfer of functions) – will commence on a day to be fixed by Proclamation.

Schedule 6 (Other amendments) – will commence on the day on which this Act receives Royal Assent or as otherwise specified by this Bill.

Clause 3: Schedule(s)

This clause provides that each Act that is specified in a Schedule is amended or repealed as set out in that Schedule.

Schedule 1 – Stored communications

Part 1 – Principal Amendments

The purpose of this Part is to introduce a warrant regime for enforcement agencies to access stored communications held by a telecommunications carrier. The Blunn Report recommended that:

- (a) the distinction between real time access i.e. interception, and access to stored data be maintained;
- (b) access to stored communications continue to be authorised by search warrant but those warrants be required to meet minimum prescribed standards; and
- (c) in the context of accessing stored communications any specific reference to Voice over Internet Protocol (VoIP) is unnecessary and should be removed.

The amendments create a general prohibition on access to stored communications held by a telecommunications carrier, subject to limited exceptions. The primary exception is for access by enforcement agencies subject to a stored communications warrant.

A stored communications warrant will be available to an enforcement agency that is investigating an offence punishable by a maximum period of imprisonment of at least three years, or a pecuniary penalty of at least 180 penalty units.

The amendments regulate the use, communication and recording of information obtained by accessing stored communications, and require enforcement agencies to report to the Minister regarding the use of stored communications powers. Information obtained by accessing stored communications can only be used or communicated for a purpose in connection with the investigation of an offence that is punishable by a maximum period of imprisonment of at least one year, or a pecuniary penalty of at least 60 penalty units.

Significantly, the prohibition against accessing stored communications is limited to those communications accessed from a telecommunications carrier. This limitation gives express recognition to the ability of enforcement agencies to continue to use existing lawful access arrangements where access is to be obtained via the person of interest or relevant premises. For example, the amendments do not alter an enforcement agency's ability to access stored communications held on a person's computer or mobile telephone where that agency has lawful access to the mobile handset or computer terminal. Enforcement officer's will continue to have lawful access to a mobile handset where the person is in lawful custody, and will have lawful access to stored communications held on a person's computer subject to a lawfully issued general search warrant. Similarly, notices to compel disclosure of information may still be utilised for access to stored communications by enforcement agencies such as the Australian Competition and Consumer Commission or the Australian Securities and Investments Commission where the use of the notices is overt.

Item 1

Item 1 inserts a definition of *stored communication* into subsection 5(1) of the Act. A stored communications is defined to mean a communication with four specific elements:

- First, the communication must have passed over a telecommunications system. This is to ensure that the stored communications regime does not apply to communications that have been prepared but have not been sent (such as drafted emails).
- Second, the communication must not be passing over that or any other telecommunications system. This is to ensure that a communication is only a stored communication once it has ceased passing over a telecommunications system, which is subject to the prohibition against interception in subsection 7(1) of the Act. New section 5F further clarifies the concept of passing over a telecommunications system.
- Third, the communication must be held on equipment operated by the carrier at its premises. This is to ensure that, as noted above, 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 telecommunications device.
- Finally, the communication must be accessible to the intended recipient of the communication. This further clarifies when a communication has ceased passing over a telecommunications system, by ensuring that the stored communications regime only applies to communications that the intended recipient is able to access. New section 5G defines intended recipient of a communication and new section 5H further clarifies when an intended recipient is able to access a communication.

Item 2

Item 2 inserts four new definitional sections into the Act.

New section 5E

New section 5E defines *serious contravention*, which must be, or have been, committed, or be reasonably suspected of being committed (see new subsection 5E(2)) for an enforcement agency to be able to obtain a stored communications warrant.

New subsection 5E(1) defines serious contravention to be a contravention against a law of the Commonwealth, a State or a Territory that is:

- a serious offence (the existing threshold for obtaining a telecommunications interception warrant, as defined by section 5D);

- an offence punishable by imprisonment for a period, or a maximum period, of at least three years, or the equivalent pecuniary penalty (which is at least 180 penalty units for individuals or at least 900 penalty units for corporations); or
- a breach of a civil penalty provision that would render the person committing the contravention liable to a fine of at least 180 penalty units (or at least 900 units if the person is a corporation).

In accordance with section 4AA of the *Crimes Act 1914*, 180 penalty units is equivalent to \$19,800 and 900 penalty units is equivalent to \$99,000.

New section 5F

New section 5F defines the concept of passing over a telecommunications system. It clarifies that a communication that is passing over a telecommunications system continues to do so until it can be accessed by the intended recipient of the communication. New section 5G defines intended recipient of a communication and new section 5H further clarifies when an intended recipient is able to access a communication.

This definition also applies to the interception of telecommunications, as both section 6, in defining interception, and section 7, in prohibiting interception of telecommunications, refer to communications passing over a telecommunications system. This definition ensures that communications that are accessible to the intended recipient are no longer passing over a telecommunications system and are not subject to the general prohibition on interception.

Communications that are passing over the telecommunications system remain subject to the prohibition against interception. Communications that are stored communications are subject to the new prohibition against access to stored communications. Communications that have ceased passing over the telecommunications system and are not stored communications (because they are not accessed via the carrier) remain subject to general lawful access including consent, general search warrant, notices to produce.

New section 5G

New section 5G defines *intended recipient* as follows:

- First, where the communication is addressed to a person who is an individual, the intended recipient is that individual. This definition applies whether the individual is acting in his or her own capacity or as the employee or agent of another. This ensures that where the communication is sent to the individual via an address (such as an email address) that is a work address, it is intended to be sent to the individual.
- Second, where the communication is addressed to a person who is not an individual, the intended recipient is that person. This definition applies when the communication is sent to a corporation, partnership, association or other group of persons, without any identification of any particular individual. In

this case, the intended recipient is the group itself, and therefore any person within it who is able to access communications sent via that address.

- Finally, where the communication is not addressed to a person, the intended recipient is any person, or any employee or agent of the person, who has control over the telecommunications service to which the communication was sent. This definition applies when the communication is sent to a generic address (such as an email address), where the person sending the communication does not identify a specific person or group of persons. In this case, the intended recipient is any person who has access to communications sent to that address.

New section 5H

New section 5H defines the concept of when a communication is accessible to the intended recipient.

New subsection 5H(1) provides that a communication is accessible to the intended recipient when it has been received by or has been delivered to the telecommunications service of the intended recipient, or is under the control of the intended recipient. New subsection 5H(2) ensures that new subsection (1) is not a prescriptive definition, and therefore does not limit the circumstances in which a communication is accessible to the intended recipient.

This definition is intended to be read broadly, to ensure that a communication is a stored communication even if the intended recipient has not obtained the content of the communication or is not even aware that the communication exists.

‘Accessible’ simply means that the communication is available to the intended recipient via their telecommunications device. It does not require that the intended recipient has read or listened to the communication, nor does it require the intended recipient to be aware of its existence. For example, an e-mail that is delivered to the inbox of an intended recipient is accessible even if the person is unaware of its presence or indeed not physically able to access the communication.

Item 3

Item 3 inserts new section 6AA into the Act, which defines the concept of *accessing* a stored communication to mean listening to, reading or recording a stored communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient.

The reference to the knowledge of the intended recipient is designed to protect the privacy of the communication before such time as the communication becomes accessible to the intended recipient. The requirement for knowledge also preserves the ability of law enforcement agencies to access stored communications held by a carrier where they do so with the knowledge of the intended recipient. For example, an enforcement agency may use its existing notice to produce at the carrier where they have notified the intended recipient that they intend to access the communications in this manner. This distinction means that enforcement agencies are regulated by the stored communications regime only when they are acting covertly in

the access to these communications. When acting overtly, existing access and compulsion powers of the enforcement agencies remain applicable.

The reference to ‘by means of equipment operated by a carrier’ reinforces the fact that the prohibition on accessing stored communications only relates to accessing these communications via the carrier.

In all other aspects, this definition is based on the definition of intercepting a communication in section 6 of the Act.

Item 4

This item inserts a new section 6DB into the Act which provides that the Minister responsible for the administration of the Act can, by writing, appoint as an *issuing authority* a judge of the federal court, including a judge of the Federal Court of Australia, Family Court of Australia or a Federal Magistrate, or a magistrate where those persons have consented in writing to be appointed as an issuing authority.

The amendment will also allow the Minister to appoint a person who holds an appointment to the Administrative Appeals Tribunal as Deputy President, full-time senior member, part-time senior member or member (including a part-time or full-time member), who is enrolled, and has been enrolled for at least 5 years, as a legal practitioner of a federal court or of the Supreme Court of a State or Territory.

Item 5

This item inserts new section 6EB into Part 1A of the Act, which defines *stored communications warrant information* to mean information about an application for, the issue of, the existence or non-existence of, or the expiry of a stored communications warrant, or any other information which is likely to identify the telecommunications service, or the person of interest, to which a stored communications relates. Stored communications warrant information is subject to a general prohibition against disclosure in new section 133 of the Act.

This definition is based on the definition of designated warrant information in section 6E and is designed to ensure that information about agency investigations is not disclosed.

Item 6

This item inserts a new subsection 9(1A) which will allow the Australian Security Intelligence Organisation (the Organisation) to access stored communications, in the same manner it is able to intercept communications under a telecommunications service warrant under the warrant regime in existing Chapter 2 of the Act.

Item 7

This item inserts a new subsection 9A(1A) which will allow the Organisation to access stored communications, in the same manner it is able to intercept communications under a named person warrant under the warrant regime in existing Chapter 2 of the Act.

Item 8

This item inserts a new subsection 10(1A) which will allow the Organisation to access stored communications, in the same manner it is able to intercept communications under a warrant issued by the Director-General of Security in the emergency circumstances to which section 10 of the Act apply.

Item 9

This item introduces new Chapter 3 into the Act, which establishes the general prohibition on accessing stored communications, the warrant regime exception for enforcement agencies and the accountability and oversight mechanisms.

With the introduction of the stored communications regime, the Act is to be restructured into Chapters to deal with interception and stored communications separately. Part 2 of Schedule 1 to the Bill contains many technical amendments to the Act to reflect this new structure.

New Chapter 3, dealing with the new stored communications provisions, contains seven Parts:

- Prohibition on access to stored communications
- Access by the Organisation to stored communications
- Access by enforcement agencies to stored communications
- Dealing with accessed information
- Keeping and inspection of access records
- Reports about access to stored communications
- Civil remedies

Part 3-1 – Prohibition on access to stored communications

New Part 3-1 creates a general prohibition on access to stored communications and includes a number of exceptions to this general prohibition. The structure of this Part is similar to the interception provisions of the Act, which contain the general prohibition on the interception of telecommunications.

In relation to both telecommunications interception and access to stored communications, the Act makes clear that the general position is that these activities are prohibited, except in certain clearly defined situations. This reflects the primary focus of the Act which is to protect the privacy of communications.

New section 108

New section 108 creates a general prohibition on access to stored communications reinforced by an offence, punishable by imprisonment for up to two years or a fine of

120 penalty units or both, of accessing a stored communication without the knowledge of the intended recipient of the communication. The offence extends to accessing that communication, authorising, suffering or permitting another person to access that communication, or doing any act or thing which enables another person to access a stored communication.

This offence reflects the offence of intercepting a communication as set out in section 7, while reiterating the requirement that the conduct be done without the knowledge of the intended recipient. Importantly, the penalty for the commission of this offence is the same as the penalty for the unlawful interception of a communication, illustrating that the unauthorised access of the content of a person's communication is equally serious, regardless of the method of access.

The note to new subsection (1) reiterates that this offence does not prohibit lawful access to communications from the intended recipient or stored on a telecommunications device possessed or owned by the intended recipient, ensuring that the stored communications regime only applies to accessing a communication from the carrier.

New subsection 108(2) sets out a number of exceptions to this general prohibition:

- First, where the access is authorised by a stored communications warrant. This is the most important exception which permits enforcement agency access to these communications in accordance with the new stored communications warrant regime.
- Second, where the access is authorised by an interception warrant. This exception ensures that where an enforcement agency obtains an interception warrant, it is able to gain access to all stored communications currently held by the carrier. In the absence of this exception, interception warrants, which only operate prospectively from the time they are served on the carrier, would not authorise access to stored communications previously sent, meaning that the agency would need to also obtain a stored communications warrant to ensure complete access to all communications.
- Third, where the conduct is done pursuant to a warrant issued under section 25A of the *Australian Security and Intelligence Organisation Act 1979* a computer access warrant may give access to stored communications.
- Fourth, where the conduct is done by an employee of a carrier in the course of his or her duties, where that conduct is reasonably necessary to perform those duties effectively.
- Fifth, where the conduct is done by a person as part of the installation, connection or maintenance of equipment, where that conduct is reasonably necessary to perform those duties effectively. 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.

- Sixth, where the conduct is done by a person as part of the installation, connection or maintenance of equipment to be used to access stored communications under a stored communications or interception warrant, where that conduct is reasonably necessary to perform those duties effectively. This and the previous two exceptions ensure that a carrier, or an employee or agent of a carrier, is not unlawfully accessing stored communications when such access is required to carry out his or her duties in a reasonable manner.
- Finally, where the access results from, or is incidental to, the actions of an employee of the Australian Security Intelligence Organisation (the Organisation), in lawfully determining the existence and location of a particular listening device.

These exceptions reflect, insofar as the comparison can be made, the exceptions to the offence of intercepting telecommunications as set out in section 7.

New subsection 108(3) clarifies that an interception warrant only authorises access to stored communications (the exception set out in new paragraph (2)(b)), where the interception of the communication would have been authorised by the interception warrant, had that warrant been in effect at the time the communication was sent.

The effect of this provision is to ensure that, in terms of accessing stored communications, there is no difference between an interception warrant and a stored communications warrant. This is considered appropriate as the agency has met the higher threshold needed to obtain the interception warrant, but it would be administratively burdensome for them to also have to obtain a stored communications warrant.

New subsection 108(4) provides that, in determining whether conduct was reasonably necessary for a person to perform his or her duties effectively, a court is to have regard to such matters (if any) as are specified in the regulations. This provision reflects subsection 7(2A) in relation to the interception of communications.

New Part 3-2 – Access by the Organisation to stored communications

The Australian Security Intelligence Organisation (the Organisation) is able to intercept communications under the warrant regime in existing Chapter 2 of the Act. This regime provides that the Attorney-General may issue warrants to the Organisation to intercept communications where the communications are being used by a person who is reasonably suspected of engaging in activities prejudicial to security, and the interception will, or is likely to, assist the Organisation in its function of obtaining intelligence relevant to security.

Any new warrant regime which would permit the Organisation to access stored communications would still require the Attorney-General to be the issuing authority, would still need to have the person of interest reasonably suspected of engaging in activities prejudicial to security and would still need to be likely to assist the Organisation in its function of obtaining intelligence relevant to security. As this is the same threshold as is currently required for an interception warrant, and

interception warrants permit access to stored communications, there is no need for a separate stored communications warrant for the benefit of the Organisation.

New section 109

The new section 109 ensures that the Organisation is able to use its existing telecommunications interception warrants to obtain access to stored communications.

New Part 3-3 – Access by enforcement agencies to stored communications

New Part 3-3 sets out the warrant regime for enforcement agencies to access stored communications. The provisions reflect the provisions of existing Part VI of Chapter 2 of the Act which permit law enforcement agencies to intercept telecommunications.

Unlike the Organisation, enforcement agencies will obtain a clear benefit from a separate warrant regime to access stored communications. Some of the differences include:

- Additional agencies can obtain access. Only law enforcement agencies, being those agencies specifically tasked to investigate criminal matters (including the Australian Federal Police, the Australian Crime Commission, the Police Forces of each State and Territory, and various other criminal investigatory bodies investigating serious crime and corruption), are able to obtain interception warrants. However, stored communications warrants may be accessed by all enforcement agencies as defined in section 282 of the *Telecommunications Act 1997*, which includes all the law enforcement agencies, as well as 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 will include such additional Commonwealth agencies as the Australian Customs Service, the Australian Tax Office, and the Australian Securities and Investments Commission. Similar State and Territory agencies are also included.
- There is a wider range of issuing authority. Whereas interception warrants may only be issued by eligible judges or nominated AAT members, stored communications warrants may be also be issued by these authorities as well as any other Commonwealth, State or Territory judge or magistrate.
- There is a lower threshold to be met. Interception warrants are only available in relation to specified serious offences, as defined in subsection 5(1). While these are varied in terms of their penalties, the general rule is that they relate to offences with a maximum term of imprisonment of at least seven years. In contrast, stored communications warrant are available for the investigation of these serious offences as well as offences with a penalty of imprisonment for a maximum period of at least three years or a pecuniary penalty of at least 180 penalty units for individuals and at least 900 penalty units for corporations. In addition, stored communications warrants can be obtained as part of statutory civil proceedings which would render the person of interest to a pecuniary penalty of at least 180 penalty units for individuals and at least 900 penalty units for corporations. Consistent with the lower threshold, stored

communications that have been lawfully accessed can be used as part of the investigation of matters with a lower threshold (at least one year imprisonment or at least 60 penalty units for individuals (300 penalty units for corporations)).

- Reflecting the wider agency access and the lower threshold to be met, the reporting requirements for stored communications warrant are not as burdensome on the agencies as the requirements for interception. Reduced reporting requirements are also consistent with general search warrants provisions.

New Division 1 – Applications for warrants

New Division 1 of new Part 3-3 sets out the requirements for a valid application by an enforcement agency to an issuing authority for a stored communications warrant.

New sections 110 to 115

These sections reflect sections 39 to 44 in relation to interception warrants regarding the following administrative matters associated with an application for a stored communications warrant.

Who may apply for a warrant?

New section 110 provides that in the case of an interception agency, a warrant may be applied for those officers or members of the agency that may apply for a telecommunications interception warrant (see section 39 of the Act).

In relation to other enforcement agencies, an application for a stored communications warrant may be made by a chief executive officer or person acting in that position, or a person nominated by the chief executive officer.

What is the subject of the warrant?

New section 110 provides that an agency may apply for a warrant authorising access to stored communications in respect of a person. This means that stored communications are more similar to named person interception warrants than service interception warrants, in that a stored communications warrant may authorise access to stored communications in relation to more than one telecommunications service. For example, a stored communications warrant may authorise access to all SMS messages sent to and from a specified mobile telephone number and all emails sent to and from a specified email address.

What form must a stored communications warrant be in?

New section 111 provides that a stored communications warrant must be in writing unless, because of urgent circumstances, the applicant thinks it necessary to apply by telephone.

New section 112 provides that the application will state the name of the agency and applicant.

New section 113 sets out various matters to be included in an affidavit in support of an application for a stored communications warrant, including the facts or grounds on which the application is to be in force. New section 114 provides that in addition to this information, a telephone application for a stored communications warrant must include details of the urgent circumstances that led to a telephone application.

New section 115 provides the issuing authority with the power to request further information, and the form in which the further information must be given.

New Division 2 – Issuing of warrants

New Division 2 of new Part 3-3 provides the power for an issuing authority to issue a stored communications warrant, and the form, content and duration of a stored communications warrant.

New section 116

New section 116 reflects section 46 in relation to the issue of interception warrants. It provides that an issuing authority may issue a stored communications warrant if he or she is satisfied:

- that the administrative requirements set out in new sections 110 to 115 have been complied with;
- where the application was made by telephone, that the urgency of the situation justified a telephone application;
- that there are reasonable grounds for suspecting that a particular carrier holds stored communications for whom the identified person is the sender or the intended recipient;
- that information that could be obtained from those stored communications would be likely to assist in the investigation of a serious contravention; and
- having regard to the matters listed in new subsection (2), and no other matters, that a stored communications warrant should be issued. The matters listed in new subsection (2) are an exhaustive list of the matters that an issuing authority can consider, which are the same as the matters that can be considered in relation to an interception warrant. They include the impact on privacy, the gravity of the serious contravention, the likely value of the information that could be obtained and a comparison of other methods of investigation.

New subsection 116(3) clarifies that a stored communications warrant may be issued in relation to the investigation of more than one serious contravention. This is to ensure that where the information is likely to be useful to more than one investigation, this can be put to the issuing authority who can consider this in considering the gravity of the conduct.

New section 117

New section 117 clarifies what stored communications warrants authorise access to. A stored communications warrant authorises access to stored communications for persons approved under new subsection 127(2) to stored communications that came into existence before the warrant is first issued and that are still held by the carrier.

New section 118

New section 118 states the requirements for the form and content of a stored communications warrant.

New subsection 118(1) provides that a stored communications warrant must be in the prescribed form, to be included in the regulations, and must be signed by the issuing authority who issued it.

New subsection 118(2) provides that a stored communications warrant may specify conditions or restrictions relating to accessing stored communications under the warrant.

New subsection 118(3) provides that a stored communications warrant must set out short particulars of each serious contravention of which the issuing authority is satisfied justified the issuing of the warrant.

New section 119

New section 119 provides the time for which a stored communications warrant is in force. Although equivalent provisions exist for interception warrants (see subsections 49(3), (4) and (5)), the retrospective nature of stored communications as compared to the prospective nature of interception warrants means that these provisions are necessarily different.

New subsection 119(1) provides that a stored communications warrant is in force until it is first executed, or five days after the day of which it was issued, whichever occurs first.

New subsection 119(2) provides that if a stored communications warrant authorises access to communications held by different carriers, the warrant remains in force in relation to each service until it is executed by the carrier which holds the relevant stored communication, up to the maximum five day period. For example, if a stored communications warrant authorises access to communications held by carrier A and carrier B, the warrant is still in force in relation to carrier B even if it has been executed at carrier A on the first of the five days.

New subsection 119(3) provides that the issuing authority may not extend this period. As the warrant will only permit access to communications stored at the carrier at the time the warrant is executed, and there is no requirement for carriers to hold stored communications for any length of time, it is in the agencies' interest to execute the warrant as soon as possible.

New subsection 119(4) provides that the time limits set out in this section do not prevent an issuing authority from issuing a further warrant in respect of the same person, although new subsection 119(5) provides that a further warrant cannot be

sought within three days of a previous warrant being executed in respect of the same telecommunications service. In relation to the carrier A and carrier B example above, this means that a warrant cannot be sought in relation to the stored communications held by carrier A until three days after it was executed at carrier A.

This time limit is to ensure that agencies are not able to get a new stored communications warrant daily, which would undermine the separate interception warrant regime.

Division 3 – How warrants etc. are dealt with

New Division 3 of new Part 3-3 contains provisions dealing with notification and revocation of stored communications warrants.

New section 120

New section 120 sets out what must occur when a stored communications warrant is issued on a telephone application. It ensures that although the person who applies for the warrant is aware of its terms immediately, and can therefore execute as a matter of urgency, the person must ensure that the appropriate paperwork is forwarded to the issuing authority within one day. Where this does not occur, the issuing authority may revoke the warrant.

New section 121

New section 121 sets out what must occur when a stored communications warrant is issued. It provides that the chief officer of the enforcement agency to which the warrant is issued must inform the carrier in question that a warrant has been issued and provide the carrier with a copy of that warrant as soon as practicable.

New section 122

New section 122 provides that the chief officer of the enforcement agency to whom a stored communications warrant has been issued has power to revoke the warrant.

New subsection 122(1) provides that the chief officer must revoke a warrant if satisfied that the grounds on which it was issued no longer exist, and must inform any other agency who is obtaining access to communications under the warrant to be informed of the revocation.

While the period of operation of a stored communications warrant is relatively short, the ability to revoke provides enforcement agencies with the means to prevent access to stored communications where they become aware that such access would not assist the investigation.

New subsection 122(2) provides that the chief officer may revoke the warrant at any time, once he or she has informed any other agency who is obtaining access to communications under the warrant of his or her proposed revocation.

New section 123

New section 123 provides that where a warrant is revoked, the chief officer of the enforcement agency must inform the chief officer of any other agency obtaining access to communications under the warrant, and the carrier concerned, of the revocation. The chief officer must also cause a copy of the revocation instrument to be given to the carrier as soon as practicable.

New section 124

New section 124 ensures that a stored communications warrant may be authority to access all of the stored communications pertaining to a person and held by a particular carrier, even where the communications are in relation to a telecommunications service which the enforcement agency was unaware of the person's use at the time the warrant was executed.

Where a further service is subsequently identified, new subsection 124(1) provides that the chief officer of the enforcement agency must give the carrier, as soon as practicable, a description of the service which is sufficient to identify it.

New subsection 124(2) provides that if the chief officer is satisfied that it is no longer necessary to obtain access to stored communications in relation to the further service, the carrier must be informed forthwith of that decision, followed by confirmation in writing as soon as practicable.

New Division 4 – Provisions relating to the execution of warrants

New Division 4 of new Part 3-3 sets out other provisions relating to the authority conferred by warrants.

New sections 125 and 126

New section 125 makes it clear that a stored communications warrant enters into force as soon as it has been issued. However, new section 126 makes it clear that the warrant only provides access to stored communications once it has been served on the carrier.

New sections 127 and 128

New section 127 provides that the chief officer of an agency may authorise certain officers of the agency, or another agency, to exercise the authority obtained by a stored communications warrant.

New section 128 provides that persons declared by the chief officer of an agency to be designated officers may provide technical assistance to an officer of the agency exercising authority under the warrant. Further, new subsection 128(1) provides that an employee of a carrier is authorised to provide technical assistance in the execution of a stored communications warrant.

These provisions ensure that officers of the agency which has been issued with the warrant, and those employees of the carrier on which the warrant has been served, do not commit an offence by accessing stored communications in accordance with that warrant.

New sections 129 and 130

New section 129 provides that the Managing Director or secretary of a carrier may issue a written certificate setting out facts detailing the acts done by employees of the carrier in order to enable a stored communications warrant to be executed.

New section 130 provides that the chief officer of an enforcement agency may issue a written certificate setting out facts detailing the acts done by an officer of the agency in connection with the execution of a stored communications warrant or in relation to the lawful use of information obtained under the warrant.

In each provision, the written certificate is taken to be, in an exempt proceeding, *prima facie* evidence of the matters stated in the document. This ensures that employees of the carrier or the agency are not required to testify in each proceeding which relies on evidence obtained under a stored communications warrant, simply to justify that the information was lawfully obtained.

New section 131

New section 131 assists in exempt proceedings by ensuring that a certified true copy of a stored communications warrant is taken to be the original warrant for the purpose of the rules of evidence.

New section 132

New section 132 creates an offence of obstructing or hindering, without a reasonable excuse, a person acting under the authority of a stored communications warrant. The offence is punishable by imprisonment for 6 months, or 30 penalty units, or both.

New Part 3-4 – Dealing with accessed information etc.

New Part 3-4 provides a general prohibition against dealing with accessed information, except for limited permitted dealings. It also includes provisions relating to the admissibility of evidence and the destruction of records.

New Division 1 – Prohibition on dealing with accessed information

New section 133

New section 133 creates a general offence for communicating, making use of, making a record of or giving as evidence, lawfully accessed information, information obtained by accessing a stored communication in contravention of new section 108 or stored communications warrant information.

As per the offence in the interception regime, the penalty for this offence is imprisonment for two years, 120 penalty units, or both.

New subsection 133(2) provides that the remainder of new Part 3-4 contains a number of exceptions to this general prohibition.

New Division 2 – Permitted dealings with accessed information

New Division 2 of new Part 3-4 provides a number of exceptions to the general prohibition on dealing with accessed information.

New section 134

New section 134 provides that it is an exception to the prohibition on dealing with accessed information for the purposes of applying for, or being issued, a stored communications warrant, permitting inspection of stored communications warrants or making reports to the Minister about stored communications warrants.

New section 135

New section 135 provides that it is an exception to the prohibition on dealing with accessed information for an employee of a carrier to provide the information to the agency in relation to whom a warrant has been issued, to assist with the operation of a network or to assist in lawful access to a stored communication.

New section 136

New section 136 provides that exceptions to the prohibition on dealing with accessed information in connection with the performance by the Organisation of its functions.

New section 137

New section 137 provides that it is an exception to the prohibition on dealing with accessed information for the purposes of communicating information obtained by the Organisation.

New section 138

New section 138 provides that it is an exception to the prohibition on dealing with accessed information for an employee of a carrier, to communicate accessed information to an enforcement agency for the purposes of an investigation of a serious offence, and for no other purpose.

New section 139

New section 139 provides that it is an exception to the prohibition on dealing with accessed information to communicate, use or record accessed information for the purposes of an investigation by the agency of a contravention which is a serious offence, or is punishable by a maximum period of at least 12 months or by a maximum fine of at least 60 penalty units.

The effect of the provision is to enable enforcement agencies to use accessed information for any offence that is punishable by a maximum penalty of at least 12 months or a maximum fine of at least 60 penalty units. Consistent with the interception regime, this means that after enforcement agencies meet the initial higher threshold of three years, the accessed information may be used in relation to the investigation of lesser offences.

New section 140

New section 140 provides that it is an exception to the prohibition on dealing with accessed information for a person to communicate accessed information to the Attorney-General, Director of Public Prosecutions, Commissioner of the Australian Federal Police, or Chief Executive Officer of the Australian Crime Commission if the information is believed to establish that a particular offence has been committed.

The person may communicate that information to those officers if the accessed information pertains to possible contravention of the prohibition against access to stored communications, or the prohibition against communicating accessed information.

New section 141

New section 141 provides that a person who is permitted by new sections 135, 137, 138 or subsection 140(1) to communicate accessed information, may make or cause a record of the information to be made for the purposes of communicating that information.

New section 142

New section 142 provides that a recipient of information under subsection 135(4), section 139, subsection 140(2), or section 142, may communicate the information received only for the purpose for which they received it.

New section 143

New section 143 provides that it is an exception to the prohibition on dealing with accessed information to give lawfully accessed information and stored communications warrant information in evidence in an exempt proceeding.

Subsection 143(2) provides that whether accessed information is lawfully accessed will be assessed on the balance of probabilities for the purposes of subsection 143(1).

The effect of the provision is to expressly provide for those proceedings within which lawfully accessed information may be admitted in evidence. *Exempt proceeding* is defined in section 5B of the Act.

New section 144

New section 144 provides a discretion to admit unlawfully accessed stored communications information into evidence in an exempt proceeding where the accessed information was purportedly under an irregular stored communications warrant.

New subsection 144(2) provides that an irregularity is a reference to a defect or irregularity in connection with the stored communications warrant documentation or the execution of the warrant.

New section 145

New section 145 provides that once accessed information has been provided in evidence in an exempt proceeding, the information is thereafter able to be given in evidence in any proceeding.

New section 146

New section 146 provides that accessed information or stored communications warrant information may be given in proceedings for civil relief in connection with an unlawful access to stored communications or unlawful use of communication of accessed information.

New Division 3 – Admissibility of evidence

New section 147

New subsection 147(1) provides that accessed material, being accessed information or a record of accessed information, is inadmissible in evidence in a proceeding except in relation to sections 143, 144, 145, and 146.

New subsection 147(2) provides that the accessed material is admissible in a proceeding to determine the extent to which the accessed information would be admissible in a proceeding pursuant to sections 143, 144, 145 or 146.

New section 148

New subsection 148(1) provides that stored communications warrant information is inadmissible in evidence in a proceeding except in relation to sections 143, 145, and 146.

New subsection 148(2) provides that stored communications warrant information is admissible in a proceeding to determine the extent to which the accessed information would be admissible in a proceeding pursuant to sections 143, 145 or 146.

New section 149

New section 149 clarifies that nothing in this new Part makes any information or record obtained by accessing a stored communication admissible in evidence to a greater extent than it was before the enactment of this new Part.

New Division 4 – Destruction of records

New section 150

New subsection 150(1) requires the chief officer of an enforcement agency to cause the destruction of information or a record obtained by accessing a stored communication where the chief officer is satisfied that the material is no longer required in relation to the purposes of the agency referred to in new subsection 150(2).

New subsection 150(2) provides that the chief officer must provide an annual report of destruction activity to the Minister within three months of the end of each financial year.

New Part 3-5 – Keeping and inspection of access records

New Part 3-5 establishes an oversight regime for the records to be maintained by enforcement agencies in connection with the use of stored communications warrants.

New Division 1 – Keeping access records

New section 151

New section 151 requires the chief officer of an enforcement agency to cause to be kept in the agency's records, each stored communications warrant obtained by the agency, and each revocation instrument, evidentiary certificate, and authorisation in relation to the warrant. Further, the records must include particulars of the destruction of information obtained pursuant to the warrant.

New Division 2 – Inspection of access records by Ombudsman

New section 152

New section 152 provides that the Ombudsman has the function of inspecting an enforcement agency's records in order to ascertain compliance with its record-keeping obligations, and can do anything incidental or conducive to that function. The Ombudsman has the additional function of reporting to the Minister about the results of the inspections under this new Division.

New section 153

New subsections 153(1) and (2) provide that within three months of the end of each financial year the Ombudsman will report to the Minister about the inspections conducted during the financial year of an enforcement agency's stored communications records.

New subsection 153(3) provides that the Ombudsman may report to the Minister any contravention of a provision of this Act

New subsection 153(4) provides the Ombudsman with an ability to report to the Minister at any time about the results on an inspection under this new Division, and must do so if requested by the Minister.

New Subsection 153(5) obliges the Ombudsman to provide a copy of a report under subsections 153(1) or (3) to the chief officer of the relevant enforcement agency.

New section 154

New section 154 invokes the general powers of the Ombudsman in relation to inspections as provided by the *Ombudsman Act 1976*. Those powers, however, remain subject to section 133 of the Act which provides a general prohibition against dealing with accessed information or stored communications warrant information.

New section 155

New section 155 provides that the general prohibition against dealing with accessed information or stored communications warrant information does not prevent the disclosure of information to the inspecting officer for the purposes of an inspection under this new Part, nor does section 133 prevent making a record of the information for that purpose.

New section 156

New section 156 provides that an inspecting officer may use, record or communicate information for the purposes of an inspection of an enforcement agency's records despite section 133 of the Act.

New section 157

New section 157 outlines the interaction of the *Ombudsman Act 1976* with this Act.

New subsection 157(1) provides that section 11A of that Act – regarding the power of the Federal Court of Australia to determine matters of the Ombudsman's powers – does not apply to the proposed exercise of a power or function by the Ombudsman under this new Division.

New subsection 157(2) provides that section 19 of that Act – regarding annual reporting to Parliament – does not apply to any act or omission of an inspecting officer under this new Division.

New subsection 157(3) provides that subsection 35(2), (3), (4) and (8) of that Act – regarding the observation of confidentiality of inspecting officers – apply for the purposes of this Division (subject to new section 155).

New section 158

New section 158 provides that the Ombudsman may give or receive information to those State inspecting authority's that have the function of inspecting the enforcement agency's compliance with the telecommunications interception regime. The effect of this provision is to enable the Ombudsman to communicate any accessed information to a State inspecting authority if it is relevant to the performance of the State inspecting authority's functions.

New Part 3-6 – Reports about access to stored communications

New Part 3-6 imposes requirements on enforcement agency's to provide an annual report to the Minister regarding the use of stored communications warrants. This information will assist in monitoring the utility and accountability of stored communications warrant powers.

New Division 1 – Reports to the Minister

New section 159

New section 159 obliges the chief officer of an enforcement agency to provide the Minister a report on the use of stored communications warrants. The information

required is set out in new Division 2 of this Part. The report must be provided within three months after the end of each financial year.

New section 160

New section 160 provides that the Minister may seek information from the chief officer of an enforcement agency additional to that provided under new section 159. To the extent that it is practicable, the chief officer must comply with the request of the Minister.

New Division 2 – Reports by the Minister

New section 161

New section 161 requires the Minister to cause to be prepared an annual report regarding the use of stored communications warrants in each financial year. The annual report is designed to provide public and Parliamentary visibility of the use of this investigative tool by enforcement agencies.

New section 162

New section 162 sets out the information to be included in each stored communications warrant annual report.

In relation to each enforcement agency, the report is to include the statistics regarding how many stored communication warrant applications were made, and how many applications were made by telephone.

Further, the report is to provide a total figure for all enforcement agencies regarding how many stored communication warrant applications were made, how many applications were made by telephone, how many renewal applications were made, and how many stored communications warrants were issued with conditions or restrictions.

In this manner, the annual report will provide a statistical analysis of the use of stored communications warrants and will track any trends between reporting years.

New section 163

To provide visibility of the effectiveness of stored communications warrants, each annual report will provide statistics for each enforcement agency regarding the number of arrests made on the basis of accessed information or the number of proceedings that ended during the reporting year in which accessed information was used.

New Division 3 – Provisions about annual reports

New section 164

New section 164 expressly provides for Parliamentary visibility regarding the use of stored communications warrants by obliging the Minister to table the annual report before each House of the Parliament within fifteen sitting days of its preparation.

New Part 3-7 – Civil remedies

New Part 3-7 provides the same civil remedies for unlawful access to stored communications and unlawful disclosure of accessed information as are available for unlawful interception under Chapter 2 of the Act.

New section 165

New section 165 provides that an aggrieved person – a party to the communication or on behalf of whom the communication was made – may apply for civil remedial relief against a person who unlawfully accessed the relevant communication. New subsection 165(7) provides a list of orders that may be made upon application for relief. A criminal court may also provide criminal remedial relief upon application of an aggrieved person if the court convicts a person of unlawful access.

New section 165 further provides that an aggrieved person may apply for civil remedial relief for communication of the accessed information. A criminal court may also provide criminal remedial relief upon application of an aggrieved person if the court convicts a person of unlawful communication of accessed information.

New subsection 165(11) provides that the section does not apply to unlawful access that occurred as a result of a defect or irregularity in connection with the stored communications warrant documentation or the execution of the warrant.

New section 166

New section 166 provides the limitation periods in respect of remedial relief – six years after the unlawful access or unlawful communication. An application for criminal court relief must be made as soon as practicable after the conviction occurred.

New section 167

New section 167 provides that this new Part does not limit the criminal or civil liability of a person under any other law. Further, the section provides that an aggrieved person to seek remedial relief in relation to an offence arising out of this Act.

New section 168

New section 168 preserves the operation of any law of a State or Territory that is capable of operating concurrently with this Part. For example, any State or Territory legislation that seeks to regulate lawful access to communications held other than by a carrier, is preserved by the section to the extent that it is able to operate concurrently.

New section 169

New section 169 clarifies that nothing in this new Part enables an inferior court of a State or Territory to grant remedial relief that it is otherwise unable under the laws of that State or Territory to provide.

New section 170

New section 170 overrides section 19B of the *Crimes Act 1914* so that remedial relief is available from a criminal court once a defendant has been convicted of unlawful access or unlawful communication, even if the court proceeds not to record a conviction.

Part 2 – Other amendments

New Part 2 includes amendments that are consequential upon the change of name from the *Telecommunications (Interception) Act 1979* to the *Telecommunications (Interception and Access) Act 1979*.

Items 10, 13, 14, 15, 16, 17, 18, 19, 21, 22, 23 and 24

These items make amendments cross-reference within the following Acts in connection with the change of name to the *Telecommunications (Interception and Access) Act 1979*:

- *Administrative Decisions (Judicial Review) Act 1977*
- *Australian Security Intelligence Organisation Act 1979*
- *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No.2) 2004*
- *Criminal Code Act 1995*
- *Law Officers Act 1964*
- *Mutual Assistance in Criminal Matters Act 1987*
- *Surveillance Devices Act 2004*

Items 11 and 12

Items 11 and 12 expand the reference to the secrecy provisions of the Act that are included in the *Australian Crime Commission Act 2002* to include reference to the new general prohibition against dealing with accessed information.

The effect of this item is to ensure that information that is subject to new section 133 is not subject to disclosure upon request by an Examiner of the Australian Crime Commission.

Item 20

Item 20 expands the reference to the secrecy provisions of the Act that are included in schedule 3 of the *Freedom of Information Act 1982* to include reference to the new general prohibition against dealing with accessed information.

The effect of this item is to ensure that information that is subject to new section 133 is not subject to disclosure pursuant to a freedom of information request.

Item 25

This item amends the long title of the Act to read to include reference to the prohibition of access to telecommunications.

Items 26, 27 and 28

These items are technical amendments consequent upon the renaming of the Act and inclusion of the stored communications provisions.

Item 29

This item will add a new definition of *access* into subsection 5(1) of the Act. This new definition will define access, in relation to a stored communication, to mean listening to, reading or recording such a communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient of the communication as outlined in new section 6AA which is inserted by item 3 of Part 1, Schedule 1 of this Bill.

Item 30

This item will add a new definition of *accessible* into subsection 5(1) of the Act. This new definition will define accessible as having the meaning given by section 5H which is inserted by item 2 of Part 1, Schedule 1 of this Bill.

Item 31

This item will amend the definition of *agency* in subsection 5(1) of the Act to mean, for the purposes of Chapter 2, an interception agency as defined in subsection 5(1) or for the purposes of all other chapters of the Act, an interception agency or another enforcement agency, also defined by subsection 5(1).

Item 32

This item will amend the definition of *certifying officer* in subsection 5(1) of the Act to make it clear that in the case of an enforcement agency, which is not an interception agency or eligible authority, a certifying officer is the chief executive officer, or acting chief executive officer of the enforcement agency.

Item 33

This item will amend the definition of *chief officer* in subsection 5(1) of the Act to make it clear that in the case of an enforcement agency, which is not an interception agency or eligible authority, a chief officer is the chief executive officer, or acting chief executive officer of the enforcement agency.

Item 34

This item will repeal the definition of *designated warrant information* as a consequence of the amendment to insert a new definition of *interception warrant information* at item 40.

Items 35 and 66

Item 35 will add the existing definition of *emergency service facility* which is provided in subsection 6(2A), into subsection 5(1) of the Act. This amendment will be made to ensure all definitions within the Act are listed in subsection 5(1) of the Act.

Item 66 makes a consequential amendment to subsection 6(2A) as a result of the amendment in item 35.

Item 36

This item adds a new definition of *enforcement agency* into subsection 5(1) of the Act. This new definition provides that an enforcement agency has the same meaning as in section 282 of the *Telecommunications Act 1997*, and includes an interception agency and an eligible authority.

The definition of enforcement agency is used throughout Chapter 3 of the Act which applies to stored communications warrants.

Item 38

This item will add a new definition of *intended recipient* into subsection 5(1) of the Act. This new definition provides that an intended recipient for the purposes of the stored communications warrant regime in Chapter 3, has the meaning given by section 5G which is inserted into the Act by item 2 of Part 1, Schedule 1 of this Bill.

Items 39 and 53

Item 39 will add a new definition of *interception agency* into subsection 5(1) which provides that for the purposes of Part 2-6 of the Act, an interception agency is a Commonwealth agency, or an eligible authority of a State. Except for the purposes of Part 2-6, an interception agency is defined as a Commonwealth agency or an eligible authority of a State in relation to which a declaration under section 34 of the Act is in force.

Items 53 will make consequential amendments to other sections of the Act as a result of the amendment made in item 39.

Items 37, 40, 46, 60 and 73

Item 40 will add a new definition of *interception warrant* in subsection 5(1) of the Act to mean any warrant which is issued under Chapter 2 of that Act.

Items 37, 46, 60 and 73 will make consequential amendments to other provisions of the Act as a result of the amendment in item 40.

Items 41, 72, 99, 102, 104, 105, 1107, 109, 111, 113, 115, 116, 117 and 130

Item 41 will add a new definition of *interception warrant information* in subsection 5(1) of the Act as a consequent of the amendment made by item 34 of this Part which will repeal the definition of *designated warrant information*.

Items 72, 99, 102, 104, 105, 1107, 109, 111, 113, 115, 116, 117 and 130 will make consequential amendment to other sections of the Act as a result of the amendment made in item 41.

Item 42

This item will add a new definition of *issuing authority* into subsection 5(1) of the Act which has the meaning given under section 6DB as inserted by item 4 of Part 1, Schedule 1 of this Bill.

Item 43

This item will add a new definition of *lawfully accessed information* into subsection 5(1) of the Act to mean information obtained by accessing a stored communication otherwise than in contravention of the proposed subsection 108 as inserted at item 10 of Part 1, Schedule 1 of this Bill.

Item 44, 70, 98, 103, 106, 108, 110, 112, 114, 124, 126, 131, 135, 136, 137 and 138

Item 44 will add a new definition of *lawfully interception information* into subsection 5(1) of the Act which has the meaning given by section 6E of that Act.

Items 70, 98, 103, 106, 108, 110, 112, 114, 124, 126, 131, 135, 136, 137 and 138 will make consequential amendments to other provisions of the Act as a result of the amendments made in item 44.

Item 45

This item will insert the definition of *listening device* into subsection 5(1). A listening device has the same meaning as in Division 2 of Part III of the *Australian Security Intelligence Organisation Act 1979* as provided in section 6E of the Act.

Items 47, 48, 49, 50, 51, 54, 61, 65, 67, 68, 74, 75, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 100, 118, 119, 120, 121, 122, 123, 125, 127, 128, 129, 132, 133, 134, 139, 140, 141, 142, 143, 144 and 145

These items will amend certain section numbers and headings in the Act as a result of the amendments made in Parts 1 and 2 of Schedule 1 of the Bill.

Item 52

This item will insert a note under the definition of *passing over* in subsection 5(1) of the Act to make it clear that section 5F of that Act outlines when a communications is passing over a telecommunications system.

Item 55

This item will amend the definition of *prescribed offence* within subsection 5(1) of the Act to include an offence against new subsection 108(1) or new section 133 which will be inserted by item 10 of Part 1, Schedule 1 of this Bill.

Item 56

This item will add a new definition of *publicly-listed ASIO number* into subsection 5(1) of the Act which has the meaning given by subsection 6(3) of the Act.

Item 57

This item will add a new definition of *serious contravention* into subsection 5(1) of the Act. A serious contravention will have the meaning given by section 5E as inserted by item 2 of Part 1, Schedule 1 of this Bill.

Item 58

This item will add a new definition of *stored communications warrant* into subsection 5(1) of the Act. A stored communications warrant will be a warrant which is issued under Chapter 3.

Items 59, 69, 71 and 76

Item 59 will add a new definition of *stored communications information* into subsection 5(1) of the Act. Stored communications information will have the meaning given by proposed section 6EB which will be inserted in the Act by item 5 of Part 1, Schedule 1 of this Bill.

Items 69, 71 and 76 will make consequential amendments to other provisions of the Act as a result of the amendments made in item 59.

Item 62

This item amends the definition of *warrant* within subsection 5(1) of the Act to include an interception warrant, a stored communications warrant or a Part 2-5 warrant, depending on whether the term is to be used in Chapter 2, Part 2-5 or other parts of the Act.

Item 64

This item amends the definition of *exempt proceeding* within subsection 5(1) of the Act to include the meaning of exempt proceeding within Chapter 3 of the Act.

This means that an exempt proceeding for the purposes of Chapter 3 includes a reference to a proceeding by way of a prosecution for an offence punishable by imprisonment for at least a maximum period of 12 months, or by a maximum fine of at least 60 penalty units for an individual and 300 penalty units for a corporation.

It will be an exempt proceeding for the purposes of Chapter 3 if it is a proceeding for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty,

in connection with the commission of such an offence, or where it is a proceeding for the taking of evidence pursuant to section 43 of the *Extradition Act 1988*.

Further, a proceeding for the extradition of a person from a State or Territory to another State or Territory, in so far as the proceeding relates to such an offence; or a proceeding by way of a coroner's inquest if, in the opinion of the coroner, the event that is the subject of the inquest may have resulted from the commission of such an offence; or a proceeding for recovery of a pecuniary penalty for a contravention that would, if proved, render the person committing the contravention liable to a pecuniary penalty, or a maximum pecuniary penalty, of at least 60 penalty units if the contravention is committed by an individual; or if the contravention cannot be committed by an individual—a pecuniary penalty, or a maximum pecuniary penalty, of at least 300 penalty units will also be an exempt proceeding for the purposes of Chapter 3.

Schedule 2 – B-Party Interception

The purpose of this Part is to amend the telecommunications service warrant provisions of the Act to enable interception agencies to obtain telecommunications interception warrants in relation to B-Party services in limited and controlled circumstances.

The amendments provide that where an interception agency satisfies an issuing authority that all other practicable methods of identifying the telecommunications service used by the person of interest have been exhausted, or that it is not possible to intercept the telecommunications used by the person of interest, then the interception agency may intercept the telecommunications service used by another person. Interception of the so-called B-Party service will only be available where the interception agency can satisfy the issuing authority that the person being intercepted will likely be contacted on that telecommunications service by the person of interest.

B-Party interception warrants will only be available for 45 days for law enforcement agencies and 3 months for the Australian Security Intelligence Organisation. These periods are half of the periods applicable to existing telecommunications interception warrants as B-Party interception inherently involves a potential for greater privacy intrusion of persons who may not be involved in the commission of an offence.

Lawfully obtained information obtained as a result of B-Party interception will be subject to the existing destruction provisions of the Act, namely, destruction where the permitted purpose for use ceases to exist. Generally, lawfully obtained information must be destroyed unless a purpose in connection with the investigation of an offence punishable by a maximum period of imprisonment of at least three years.

Items

Item 1

Item 1 inserts a new subparagraph 9(1)(ia) into the Act which will allow the Attorney-General to issue a warrant under section 9 to the Organisation which authorises interception the means by which a person receives or sends a communications from or to another person who is engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in such activities.

Item 2 and 3

These items will insert a note after subsection 9(1) and a new subsection 9(3) which provides that the Attorney-General may issue a warrant under section 9 to the Organisation to intercept communications of a B-Party where the Organisation has demonstrated to the Attorney-General that it has exhausted all other practicable methods of identifying the telecommunications service used, or likely to be used, by the person of interest.

Items 4 and 5

These items will amend subsection 9B(3) to provide that the time period for a B-Party warrant issued to the Organisation by the Attorney-General must not exceed 3 months.

Items 6,

This item amends subsection 46(1) to provide that the preconditions in paragraphs (a) to (c) must each be separately met prior to the issue of an interception warrant.

Item 7

This item amends subsection 46(1) of the Act to provide that a telecommunications service warrant can be issued in relation to a person who is involved in the commission of an offence, or a person who communicates with such a person.

Item 8 and 9

These items insert a new subsection 46(3) which provides that an eligible judge or nominated AAT must not issue a telecommunications service warrant for a B-Party warrant unless he or she is satisfied that the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person involved in the serious offence or serious offences, or where the interception of a telecommunications service used, or likely to be used by that person is not practicable.

This means that, for example, where an undercover police operative is provided a mobile handset to communicate with the suspect by the suspect and the interception of the suspect's services is not practical because the service cannot be readily identified. The telecommunications of the undercover operative would be able to be intercepted under section 46.

Item 10

This item will amend subsection 49(3) to provide that the time period for a B-Party warrant issued to the agency by an eligible judge or nominated AAT member must not exceed 45 days.

Schedule 3 – Equipment-based interception

The purpose of this Schedule is to amend the named person telecommunications interception warrant provisions to enable interception agencies to intercept communications to and from communications equipment such as mobile handsets and computer terminals. These amendments are designed to assist interception agencies to counter measures undertaken by persons of interest to evade telecommunications interception such as adopting multiple telecommunications services.

The amendments will enable interception agencies to apply to an issuing authority for a named person warrant to intercept communications from identified telecommunications devices. An issuing authority must not authorise interception on the basis of the telecommunications device 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. The latter situation covers instances in which agencies may be able to identify all services, but it is impractical to intercept each service. For example, a person of interest may transfer hundreds of different Subscriber Identity Module (SIM) cards through a mobile handset in quick succession. Interception of each telecommunications service (currently identified by reference to the SIM card) is extremely impractical to achieve before the person of interest changes the SIM card being used.

Interception on the basis of a telecommunications device is subject to the existing reporting, disclosure and destruction provisions of the Act, and agency compliance with these accountability mechanisms are monitored by the Inspector-General of Intelligence and Security in the case of the Organisation, and the Ombudsman or equivalent State oversight agency in relation to law enforcement interception agencies.

Item 1

Item 1 amends the definition of equipment to include *telecommunications device* (see item 2).

Item 2

Item 2 inserts a definition of telecommunications device into the Act. The effect of the definition will be to enable interception of communications to or from the device subject to an interception warrant.

Telecommunications device means a terminal device capable of sending or receiving a communication via the telecommunications system. A terminal device is any end piece of telecommunications equipment by which a person may communicate, including a mobile handset, personal computer, or personal digital assistant.

Item 3

Item 3 inserts a definition of telecommunications number into the Act. The telecommunications number is a means by which interception agencies' may identify

the telecommunications device which is to be the subject of an interception warrant.

A telecommunications device may be identified by any unique number including a telephone number for mobile phone handsets, a Media Access Control address for computer terminals, or an e-mail address. The definition of telecommunications number is inclusive so as not to limit the unique numbers which may be used to identify telecommunications devices, thereby maintaining a technology neutral approach to the regulation of telecommunications interception.

Item 4

Item 4 provides that a telecommunications device may be identified by a unique telecommunications number or any other unique identifying factor.

The requirement that a telecommunications number or identifying factor be unique is designed to ensure that interception only occur where an interception agency is able to identify the particular telecommunications device that is to be the subject of telecommunications interception.

Item 5

Item 5 repeals and substitutes subsection 9A(1) of the Act which provides the Attorney-General may issue a named person warrant to the Organisation for the purposes of obtaining intelligence in relation to security.

The substituted provision amends the existing subsection 9A(1) to include interception on the basis of a telecommunications device. The effect of the provision is to enable the Organisation to identify communications of a person that are to be intercepted by reference to the telecommunications device or devices operated by the particular person of interest.

Item 6

Item 6 is a saving provision designed to preserve the operation of a named person warrant obtained by the Organisation pursuant to subsection 9A(1) of the Act prior to the repeal and substitution of the subsection.

Item 7

Item 7 requires that the Director-General of Security include in an application for a warrant under section 9A a description of the telecommunications device sufficient to identify the telecommunications device used or likely to be used by the person of interest. The telecommunications device may be described by reference to a unique telecommunications number or other unique number as per new section 6Q and (see also the definition of 'telecommunications number' in subsection 5(1)).

Item 8

Item 8 inserts an additional criteria to be met in an application for a section 9A warrant made by the Organisation when seeking interception on the basis of a telecommunications device operated by the person of interest. Before issuing such a

warrant to the Organisation, the Attorney-General must be satisfied that the Organisation has no practicable methods of identifying the telecommunications service to be intercepted at the time of the application, or that interception of the telecommunications service would be impracticable.

For example, where a person of interest is using multiple SIM cards in a single mobile handset in quick succession, it is impracticable to identify the telecommunications service (by reference to a particular SIM card) to be intercepted. In that situation, interception can be affected on the basis of the telecommunications device. Accordingly, it need not be impossible for an agency to intercept on the basis of the particular service, rather there must be sufficient factors that would make it impracticable to intercept a particular service of the person of interest and interception by other means would be less effective.

Item 9

Item 9 repeals and substitutes subsection 11B(1) of the Act which provides that the Attorney-General may issue a named person warrant to the Organisation for the purposes of obtaining foreign intelligence relating to a matter specified in the notice.

The substituted provision amends the existing 11B(1) to include interception on the basis of a telecommunications device. The effect of the provision is to enable the Organisation to identify communications of a person that are to be intercepted by reference to the telecommunications device or devices operated by the particular person of interest.

Item 10

Item 10 is a transitional provision designed to preserve the operation of a named person warrant obtained by the Organisation pursuant to subsection 11B(1) of the Act prior to the repeal and substitution of the subsection.

Item 11

Item 11 requires that the Director-General of Security include in an application for a warrant under 11B a description of the telecommunications device sufficient to identify the telecommunications device used or likely to be used by the person of interest. The telecommunications device may be described by reference to a unique telecommunications number or other unique number as per new section 6Q and (see also the definition of ‘telecommunications number’ in subsection 5(1)).

Item 12

Item 12 inserts an additional criteria to be met in an application for an 11B warrant made by the Organisation when seeking interception on the basis of a telecommunications device operated by the person of interest. Before issuing such a warrant to the Organisation, the Attorney-General must be satisfied that the Organisation has no practicable methods of identifying the telecommunications service to be intercepted at the time of the application, or that interception of the telecommunications service would be impracticable. See example at item 8.

Item 13

Item 13 amends the notification requirements in section 16 of the Act to remove the requirement to identify the telecommunications service to be intercepted from applying to the named person warrants that authorise interception of telecommunications devices.

Item 14

Item 14 amends the notification requirements in section 16 of the Act to oblige a certifying person of the Organisation to provide the Managing Director of a carrier with a written description sufficient to identify any telecommunications device to be intercepted if that telecommunications device is not identified on the warrant. This provision recognises that named person warrants may authorise interception of multiple telecommunications devices.

Items 15 and 16

Item 15 amends the notification in the requirements in section 16 to oblige a certifying officer of the Organisation to inform the Managing Director of a carrier where the Director-General is satisfied that interception of a telecommunications device is no longer required.

Item 17

Item 17 amends the requirements for an affidavit that is required in support of an application by law enforcement interception agencies for a named person warrant. The effect of the provision is to require the affidavit to include a description sufficient to identify any telecommunications device to be intercepted (to the extent that these are known at the time of the application).

Item 18

Item 18 repeals and substitutes paragraph 46A(1)(d) of the Act which provides that an issuing authority may only issue a named person interception warrant where he or she is satisfied that intercepting the communications of the person would assist in the investigation of the applicant agency.

The substituted provision requires that the issuing authority be satisfied of those matters where the applicant agency seeks interception of the telecommunications services of the person or the telecommunications devices of the person.

Item 19

Item 19 inserts a note highlighting that a named person warrant issued under subsection 46A(1) is subject to the additional restrictions in subsection 46A(3) (see item 21).

Item 20

Item 20 repeals and substitutes paragraph 46A(2)(a) of the Act which requires the

issuing authority to have regard to the interference with the privacy of the person of interest by authorising interception of the person's services.

The substituted provision requires the issuing authority to have regard to the interference with the privacy of the person of interest that will be caused by authorising the interception of the person of interest's telecommunications services or telecommunications devices.

Item 21

Item 21 inserts an additional criteria to be met in an application for a named person warrant made by an interception agency when seeking interception on the basis of a telecommunications device operated by the person of interest. Before issuing such a warrant, the issuing authority must be satisfied that the applicant agency has no practicable methods of identifying the telecommunications service to be intercepted at the time of the application, or that interception of the telecommunications service would be impracticable. See example at item 7.

Item 22

Item 22 amends the notification requirements in section 60 of the Act to remove the requirement to identify the telecommunications service to be intercepted from applying to the named person warrants that authorisation interception of telecommunications devices.

Item 23

Item 23 amends the notification requirements in section 60 of the Act to oblige a certifying person to provide the Managing Director of a carrier with a written description sufficient to identify any telecommunications device to be intercepted if that telecommunications device is not identified on the warrant. This provision recognises that named person warrants may authorise interception of multiple telecommunications devices.

Item 24

Item 24 amends the notification in the requirements in section 60 to oblige a chief officer or certifying officer to inform the Managing Director of a carrier where the chief officer or certifying officer is satisfied that interception of a telecommunications device is no longer required.

Schedule 4 – Class 1 and Class 2 offences

The purpose of this Part is to remove the distinction between class 1 and class 2 offences and to redefine the offences for which law enforcement agencies may apply for an interception warrants, including telecommunications service warrants and named person warrants. The offences will be redefined as serious offences.

The amendment will require the issuing of all interception warrants to have regard to privacy considerations. Previously, only class 2 interception warrants required an eligible judge or nominated AAT member to have regard to the privacy considerations.

These amendments are designed to simplify a complex area of the interception regime and enhance the privacy underpinnings of the Act.

Items 1 and 2

Items 1 and 2 repeal the definitions of class 1 and class 2 offences in subsection 5(1) to reflect the insertion of a new definition of serious offence. The new definition of serious offence will incorporate all offences defined as class 1 and class 2 offences.

Item 3

Item 3 removes the reference to section 45A within the definition of named person warrants in subsection 5(1) as a consequence of repealing section 45A at item 17.

Item 4

Item 4 removes references to class 1 and class 2 offences within the definition of prescribed offence and substitutes the new description of serious offence in subsection 5(1).

Item 5

Item 5 amends the definition of serious offence within subsection 5(1) to include the previous definitions of class 1 and class 2 offences.

Item 6

Item 6 removes the reference to section 45 within the definition of telecommunications service warrant in subsection 5(1) as a consequence of repealing section 45 at item 17.

Item 7

Item 7 inserts the previous definition of class 1 offence in subsection 5D(1) and redefines class 1 offences as serious offences.

Items 8, 9, 11, and 12

Items 8, 9, 11, and 12 remove the reference to class 2 offence in subsections 5D(2), (2A), (3), (3A), (4), (5), (5A), and (6) and substitutes the new reference to serious offence in its place.

Item 10

Item 10 amends subsection 5D(5A) to remove a duplicated reference to Division 307 of the *Criminal Code Act 1995* due to the merging of the definitions of class 1 and class 2 offence to a single definition of serious offence.

Item 13

Item 13 inserts a new subsection 5D(7) which ensures that it is a serious offence for the purposes of the interception regime if an offence is constituted by receiving or assisting a person who is, to the offender's knowledge, guilty of a serious offence, which was previously a class 1 offence as outlined in subsection 5D(1), in order to enable the person to escape punishment or to dispose of the proceeds of the offence.

Item 14

Item 14 repeals and substitutes paragraph 6H(a) to remove references to section 45 as a consequence of repealing section 45 at item 17.

Item 15

Item 15 repeals and substitutes paragraph 6H(b) to remove references to section 45(c) and (d), and 45A(c) and (d) as a consequence of repealing sections 45 and 45A at item 17.

Item 16

Item 16 repeals and substitutes subsection 7(9) to replace references to class 1 or class 2 offences with the new definition of serious offence.

Item 17

Item 17 repeals sections 45 and 45A. These sections provide for the issuing of telecommunication service warrants and named person warrants for class 1 offences. As Schedule 5 of this Bill amends the Act to remove the distinction between class 1 and class 2 offences, and redefines those offences as serious offences to which the amended sections 46 and 46A apply, there is no longer a need to maintain sections 45 and 45A.

Item 18

Item 18 replaces references to class 2 offences with the new reference to serious offence within paragraphs 46(1)(d) and 46A(1)(d). The effect of this amendment is that all telecommunication service warrants and named person warrants for serious offences will be issued under sections 46 and 46A.

Items 19, 20, 21 and 22

Items 19, 20, 21 and 22 amend section 47, subsection 48(1), paragraph 48(3)(c) and subparagraph 48(3)(d)(ii) to remove references to section 45 as that section will be repealed by item 17.

Item 23

Item 23 amends paragraph 49(7)(a) to substitute references to class 1 and class 2 offences with serious offence and to remove references to section 45 as that section will be repealed by item 17.

Item 24

Item 24 amends paragraph 49(7)(b) to remove references to paragraph 45(d) and 45A(d) as those paragraphs will be repealed by item 19.

Items 25 and 26

Items 25 and 26 amend subsections 54(1) and 61(3) to remove references to sections 45 and 45A which will be repealed by item 17.

Item 27

Item 27 amends subparagraph 81A(2)(g)(i) to substitute references to class 1 and class 2 offences with serious offence and to remove references to section 45 as that section will be repealed by item 17.

Item 28

Item 28 amends subparagraph 81A(2)(g)(ii) to remove references to paragraph 45(d) and 45A(d) as those paragraphs will be repealed by item 17.

Item 29

Item 29 amends subparagraph 81C(2)(g)(i) to substitute references to class 1 and class 2 offences with serious offence and to remove references to section 45 as that section will be repealed by item 17.

Item 30

Item 30 amends subparagraph 81C(2)(g)(ii) to remove references to paragraph 45(d) and 45A(d) as those paragraphs will be repealed by item 17.

Part 2 – Transitional provisions**Item 31**

Item 31 is a transitional provision in relation to applications for interception warrants. The effect of this provision is that pending warrant applications made under section 45 prior to the commencement of this Schedule will continue in force as if they were made under section 46 after the commencement of this Schedule. Similarly, pending warrant applications pursuant to old section 45A will continue in force as if made under section 46A after the commencement of this Schedule.

Item 32

Item 32 is a transitional provision that saves the operation of sections 45 and 45A warrants. The effect of this item is that section 45 and 45A warrants will continue as if issued under section 46 and 46A respectively after the commencement of this Schedule.

Item 33

The effect of item 33 is to preserve the validity of warrants issued under sections 46, 46A and 48 despite the changes made to those provisions by the Schedule.

Item 34

Item 34 is a transitional provision that enables a warrant under section 46 or 46A to be issued as renewal warrants for existing 45 or 45A warrants after the commencement of this Schedule.

Schedule 5 – Transfer of functions

The purpose of this Schedule is to repeal the Telecommunications Interception Remote Authority Connection (TIRAC) function exercised by the Telecommunications Interception Division of the Australian Federal Police (AFP) and related provisions from the operation of the Act.

The Blunn Report recommended the removal of the TIRAC function from the Act.

TIRAC is 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 they 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. TIRAC's utility has been exhausted by technological developments, and it is therefore proposed that it be removed from the Act.

The proposed amendments will continue to require all agencies to maintain comprehensive records as part of the interception regime, however, interception agencies will no longer be required to notify the AFP of the issue of the warrant before it takes effect.

The proposed amendments also transfer the function of compiling the registers to the Secretary of the Attorney-General's Department. Greater real time accountability than is currently provided would be achieved by requiring the Secretary of the Department to receive and review warrants immediately upon issue, and maintenance of the warrant registers for the Attorney-General's quarterly inspection as already required under the Act.

Items

Item 1

Item 1 amends the definition of permitted purpose by replacing the reference to the Chief Executive Officer of the Australian Crime Commission with a reference to the chief executive officer of a Commonwealth agency. The effect of the amendment is to permit use and disclosure of intercepted material for Commonwealth agencies for record-keeping purposes. This is an existing permitted purpose which has been restated in consequence to the amendments to the record-keeping requirements in item 23.

Item 2

Item 2 repeals Division 1 of Part VI of the Act which refers to the Telecommunications Interception Division (TID) of the AFP. Once the express function of TIRAC has been removed from the AFP, there is no need to expressly refer to the TID.

Item 3

Item 3 updates a reference to the record-keeping requirements in consequence to the amendments to the record-keeping requirements in item 23.

Item 4

Item 4 amends section 47 to provide that an interception warrant issued under sections 46 or 46A does not authorise the interception of communications unless notification of the issue of the warrant has been received by or on behalf of the Managing Director of a carrier under subsection 60(1), and the interception takes place as a result of action taken by an employee of the carrier.

Item 5

Item 5 removes the reference to the AFP in subsection 52(2). The effect of the item is to notify the Secretary of the Department of a proposed revocation and provide a copy of that revocation to the Secretary of the Department.

Item 6

Item 6 amends paragraphs 52(2)(a) and (b) to transfer the requirement to notify the Commissioner of Police about the issue of an interception warrant to the Secretary of the Department.

Item 7

Item 7 omits reference to the AFP in subsection 53(1) thereby requiring all interception agencies, including the AFP to notify the Secretary of the Department of the issue of a telecommunications interception warrant.

Item 8

Item 8 amends paragraphs 53(1)(a), (b) and (c) to transfer the requirement to notify the Commissioner of Police about the issue of an interception warrant to the Secretary of the Department.

Item 9

Item 9 repeals and substitutes section 54 to provide that a warrant comes into force when it is issued.

Item 10

Item 10 repeals section 56. This section is made redundant with the removal of the TIRAC function from the Act.

Items 11 and 12

Items 11 and 12 amend subsections 57(1) and (2), and paragraphs 57(3)(a) and (b) to transfer the requirement to notify the Commissioner of Police regarding the revocation of a warrant to the Secretary of the Department.

Item 13

Item 13 adds in a new subsection 57(5) which provides that the requirements to notify the Secretary of the Department about the revocation of a warrant contained in section

57 do not apply in relation to a warrant that has ceased to be in force as the Commissioner of Police would have been notified in accordance with the previous, now repealed, requirements of section 57.

Item 14

Item 14 repeals and substitutes subsection 58(1) to amend the discontinuance provisions in consequence to the amendments to the notification requirements in connection with the removal of the TIRAC function.

Item 15

Item 15 amends subsection 58(2) to remove the reference to the now repealed subsection 56(2).

Item 16 and 17

Items 16 and 17 amend section 59 and paragraph 60(2)(a) to transfer the requirement to notify the Commission of Police regarding the revocation of a warrant to the Secretary of the Department.

Items 18 and 19

Item 18 repeals subsection 61(3) as the removal of the TIRAC function from the Act makes the issuing of evidential certificates about the enabling of a warrant as part of the TIRAC function redundant. In order to implement this removal of this requirement, item 19 provides that a certificate issued under subsection 61(3) of the Act that had effect immediately before the repeal of subsection 61(3) by this Bill, has effect after that repeal as if that subsection had not been repealed.

Item 20

Item 20 omits reference to subsection 61(3) in consequence of the repeal of that subsection at item 18.

Item 21

Item 21 amends subsection 79(2) to take into account the amendments which transfer responsibility for the maintenance of the warrant registers from the Commission of Police to the Secretary of the Department.

Item 22

Item 22 amends the heading to Part 2-7 of the Act to reflect that the Registers will be kept by a non-interception agency, being the Secretary of the Department.

Item 23

Item 23 repeals and substitutes the record-keeping requirements in sections 80 and 81 to remove reference to notifications previously provided to the Commissioner of Police.

Item 24

Item 24 amends subsections 81A(1) and (2) to take into account the amendments which transfer responsibility for the maintenance of the warrant registers from the Commission of Police to the Secretary of the Department.

Item 25

Item 25 is a saving provision which preserves the General Register of Warrants maintained by the Commissioner of Police as the General Register of Warrants maintained by the Secretary of the Department after the commencement of this item.

Item 26

Item 26 repeals and substitutes subsection 81B(1) to update the reference to the commencement of the provision. The effect of the provision is to require the Secretary of the Department to provide the General Register to the Minister for inspection within 3 months of the commencement of this Act.

Items 27 and 28

Items 27 and 28 amends subsections 81B(2), 81C(1) and (2) to take into account the amendments which transfer responsibility for the maintenance of the warrant registers from the Commission of Police to the Secretary of the Department.

Item 29

Item 29 is a saving provision which preserves the Special Register of Warrants maintained by the Commissioner of Police as the Special Register of Warrants maintained by the Secretary of the Department after the commencement of this item.

Item 30

Item 30 repeals and substitutes subsection 81D(1) to update the reference to the commencement of the provision. The effect of the provision is to require the Secretary of the Department to provide the Special Register to the Minister for inspection within 3 months of the commencement of this Act.

Items 31, 32 and 33

Items 31, 32 and 33 amends subsections 81D(2), (3) and 81E(2) to take into account the amendments which transfer responsibility for the maintenance of the warrant registers from the Commission of Police to the Secretary of the Department.

Item 34

Item 34 is a saving provision for any notice issued before the commencement of this schedule by the Commissioner of Police seeking further information for use in the compilation of the registers. Those notices will continue in force as if issued by the Secretary of the Department.

Item 35

Item 35 removes the need for the Ombudsman to inspect the maintenance of the registers of warrants as the registers will no longer be maintained by the AFP.

Schedule 6 – Other amendments

The purpose of this Schedule is to make other necessary amendments to the Act to ensure the ongoing effective operation of the interception regime in Australia.

These amendments will amend the Act to

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

Item 1

Item 1 will amend the definition of permitted purpose of the Act by amending subparagraph 5(1)(f)(ii). A permitted purpose in the case of the Office of Police Integrity will mean a purpose connected with an investigation by the Director, Police Integrity under the Police Regulation Act or the Whistleblowers Protection Act, into serious misconduct (which includes corrupt conduct), together with any report on such an investigation.

This means that, under section 67 of the Act, the Director, Police Integrity may disclose lawfully intercepted information to another person but only for a purpose connected with an investigation by the Director, Police Integrity under the Police Regulation Act or the Whistleblowers Protection Act into the conduct of a member of the force or into serious misconduct (which includes corrupt conduct), together with any report on such an investigation.

Item 2

Item 2 will amend the definition of prescribed offence of the Act to correct a previous drafting error by inserting an ‘or’ at the end of paragraphs 5(1)(a), (b) and (c).

Item 3

Item 3 will add a new definition to subsection 5(1) of the Act for the **Whistleblowers Protection Act** to mean the *Whistleblowers Protection Act 2001* of Victoria.

Item 4

Item 4 amends paragraph 5D(4) to update the reference to the New South Wales money laundering offences to which an interception agency can apply for an

interception warrant. Due to a legislative change in New South Wales, the money laundering offences were relocated from the *Confiscation of Proceeds of Crime Act 1989* (NSW) into the *Crimes Act 1900* (NSW).

Item 5

Item 5 will repeal subsection 6(2). Section 6(2) creates an exception to the general prohibition in subsection 7(1) against the interception of a communication in its passage over the Australian telecommunications system.

At the commencement of the Act, subsection 6(2) was intended to exempt the activities of telecommunications carriers and employees of carrier from the general prohibition contained in subsection 7(1) to allow the testing of the carrier's equipment to ensure that the telecommunications network and associated equipment operated correctly. However, the operation of subsection 6(2) has become redundant in the deregulated and rapidly changing telecommunications environment. Further, the continued application of subsection 6(2) undermines the strict privacy protections contained in the Act because it may allow for participant monitoring. That mean, that the continued application of subsection 6(2) allows a person who is lawfully on the premises to which the telecommunications service is provided, to listen to or record all communications when using an apparatus or equipment that is part of that telecommunications service, even where there is no knowledge of the parties to the communication.

This amendment is required as subsection 6(2) no longer has application in the deregulated telecommunications market and its continued application undermines the strict privacy protections contained in the Act is based.

Item 6

Item 6 will repeal subsection 7(11) of the Act. This amendment is required as a consequence of repealing subsection 6(2) of the Act as explained at item 5.

Item 7

Item 7 will amend subsection 12(1) of the Act to correct a drafting error. This amendment will remove the subsection number as it is not necessary because there are no other subsections in section 12.

Item 8

This item will amend subsection 55(5) of the Act to make it clear that an employee of a carrier can provide technical assistance to a law enforcement agency, or officer, when such an agency or officer is executing an interception warrant on a carrier and throughout the consequent interception.

This amendment was necessary in light of the decision of the South Australian District Court in the case of *R v Sutton and Rodgers* (Simpson J, District Court of South Australia, Unreported 10 February 2003).

This amendment will have retrospective commencement to ensure the validity of the provision of technical assistance by an employee of a carrier since the commencement of the Act.

Item 9

This item will amend section 78 to remove the reference to Part IIA within the section. This amendment is necessary to correct a drafting error as Part IIA was repealed by the *Telecommunications (Interception) Amendment Act 1993* and no longer as application.

Item 10

Item 10 will amend paragraphs 81C(3)(a) and 4(a) to add the words ‘has been issued’ at the end of both those paragraphs. This amendment is necessary to correct a drafting error and to ensure a clear reading of section 81C.