2002-2003-2004

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

SURVEILLANCE DEVICES BILL 2004

EXPLANATORY MEMORANDUM

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

SURVEILLANCE DEVICES BILL 2004

GENERAL OUTLINE

The Surveillance Devices Bill 2004 will add to and strengthen a legislative regime which has consisted of a piecemeal combination of State and Commonwealth legislation and common law principles. Legislation at a federal level, namely the Customs Act 1901 and the Australian Federal Police Act 1979, is outdated and inadequate in the face of progressively complex and covert criminal activity.

The Bill is broadly based on the model surveillance device laws developed by the Joint Working Group on National Investigation Powers.

The Bill does not prohibit the use of surveillance devices, but merely establishes a structured process for their use, where such use would ordinarily be prohibited under a State or Territory law.

Surveillances devices are data surveillance devices, listening devices, optical surveillance devices and tracking devices. Surveillance devices may be used by the AFP, the ACC and State and Territory police for the investigation of Commonwealth offences which carry a maximum penalty of at least three years imprisonment or to assist in the safe recovery of a child where the Family Court of Australia has issued a recovery order. The AFP and the ACC may also use them to investigate a State offence which has a federal aspect which meets the three year threshold.

Surveillance devices may also be used for certain offences against the Fisheries Management Act 1991, such as the illegal fishing of Patagonian tooth fish, although these offences do not carry terms of imprisonment. Surveillance devices may also be used for offences under sections 15 and 18 of the Financial Transaction Reports Act 1988 (FTR Act), which relate to the failure to declare the import or export of money in excess of A$10,000 and operating an account with a cash dealer in a false name. The FTR offences carry a two year term of imprisonment but are included in the Bill as often, they are indicative of more serious underlying conduct.

Data surveillance devices and listening devices may only be used with a warrant issued by a judge or an AAT member unless special circumstances of urgency exist involving a serious risk to a person or property, urgent circumstances relating to the recovery of a child or where there is a risk of loss of evidence for certain listed offences such as drug offences, terrorism, espionage, sexual servitude and aggravated people smuggling offences. In such cases, a member of the agency of at least SES level may issue an emergency authorisation. The use of a surveillance device under such an authorisation must be retrospectively approved by a judge or AAT member within two business days. Unless the authorisation is retrospectively approved, any information obtained under the authorisation is treated as having been illegally obtained.

Tracking devices generally also require a warrant to be issued unless the device can be installed and retrieved without entering premises, or interfering with a vehicle, without permission. In such cases a member of the law enforcement agency of at least SES level can give permission for the use of the device.

Optical surveillance devices can be used for the performance of the functions of the AFP and the ACC without a warrant in similar circumstances.

The Bill allows the use of surveillance devices for the investigation of Commonwealth offences outside Australia. With the exception of the investigation of certain offences in the contiguous and fishing zones, the consent of an appropriate official of the foreign country or the country of registration of the vessel or aircraft is required before use of the device can be lawful.

The Bill establishes a strict regime, similar to that in the Telecommunications (Interception) Act 1979, to regulate the uses to which surveillance device product is put, its communication, publication, storage, and destruction. The Bill establishes a vigorous reporting and inspection regime which allows for scrutiny of the exercise of powers under the Bill by the Ombudsman, the Attorney-General and the Parliament.

Financial Impact Statement

The Surveillance Devices Bill 2004 has expenditure implications for the Commonwealth as it enables law enforcement agencies to use a wider range of technology for the investigation of a broader range of offences. It may be that this expenditure would be offset, to some degree at least, by efficiency savings from a reduced reliance on other more labour intensive investigation methods. The Bill also imposes new inspection obligations on the Ombudsman. There may also be an increase in the number of warrants sought, particularly from the AAT.

Abbreviations used in the Explanatory Memorandum

SD	Surveillance device
TD	Tracking device
LD	Listening device
OSD	Optical surveillance device
AFP	Australian Federal Police
ACC	Australian Crime Commission
AG	Attorney-General (Cth)
ASIO	Australian Security Intelligence Organisation
TI	Telecommunications Interception
SCAG	Standing Committee of Attorney's-General
APMC	Australian Police Minister's Council
JWG	Joint Working Group
AFP Act	*Australian Federal Police Act 1979* (Cth)
Customs Act	*Customs Act 1901* (Cth)
Fisheries Act	*Fisheries Management Act 1991* (Cth)
ACT	Australian Capital Territory
NT	Northern Territory
LEA	Law Enforcement Agency
LEO	Law Enforcement Officer
FTR Act	*Financial Transaction Reports Act 1988* (Cth)
AAT	Administrative Appeals Tribunal

NOTES ON CLAUSES

PART 1 – PRELIMINARY

Clause 1 Short Title

This is a formal clause which provides for the citation of the Bill.

Clause 2 Commencement

2. The Bill commences on the day that the Act receives Royal Assent.

Clause 3 Purposes

3. This clause explains the principal objects of the Bill. The first of these is to set up a scheme which establishes the procedures for obtaining surveillance device (SD) warrants, emergency authorisations or tracking device (TD) authorisations for the installation and use of SDs in relation to criminal investigations and for locating and recovering a child in respect of whom a recovery order has been issued by the Family Court.

4. The Bill also regulates what may be done with SD product including its use, communication and publication, storage, destruction, and the making of records in connection with SD use. In this way, the Bill regulates all stages of operations which make use of SDs.

Clause 4 Relationship to other laws and matters

5. Subclause 4(1) provides that the Act is not intended to affect any other law of the Commonwealth or State or Territory that deals with SDs except where there is express provision to the contrary.

6. Subclause 4(2) provides that nothing in the Bill, except where there is express provision to the contrary, is to apply to any body, organisation or agency, however named, that is involved in the collection of information or intelligence. This provision clarifies, among other things, that this Bill does not prohibit the activity of surveillance itself. For example, the creation of a power such as the power in clause 37 does not imply that officers, employees or staff members of any other organisation or agency, such as the Australian Security Intelligence Organisation, are prohibited for using an optical surveillance device without a warrant because they are not included in this power.

7. Subclause 4(3) has been included to ensure that a court's discretion to admit or exclude evidence in any proceeding or to stay criminal proceedings in the interests of justice is not limited. Section 138 of the *Evidence Act 1995* (Cth) sets out the test for admitting improperly or illegally obtained evidence.

8. Subclause 4(4) clarifies that a warrant, emergency authorisation or TD authorisation can be issued for the installation, use, maintenance or retrieval of a SD for a relevant offence or for the enforcement of a recovery order.

Clause 5 Schedule(s)

9. This clause indicates that amendments to other legislation are set out in the Schedule.

Clause 6 Definitions

10. This clause provides the definition for many of the terms which have a particular meaning under the Act.

11. The Bill will regulate four types of SDs: listening devices (LDs), optical surveillance devices (OSDs), TDs and data surveillance devices (DSDs). In this way, the Bill allows for a range of SDs to be used that are not (with the exception of LDs) currently provided for by Commonwealth law. To ensure the definition of SD keeps pace with emerging technology, the Bill allows the types of SD covered by the Act to be added to by regulation.

12. The Bill applies to the use of SDs to Commonwealth offences, or State offences which have a federal aspect, carrying a maximum penalty of at least three years imprisonment (a 'relevant offence'). This three year threshold is in recognition of the privacy concerns raised by the use of SDs, balanced against the benefits of their use by law enforcement agencies in the investigation of serious offences

13. Offences under sections 15 and 18 of the *Financial Transaction Reports Act 1988* (FTR Act) are also 'relevant offences'. These offences relate to a failure to declare the import or export of money in excess of A$10,000 and operating an account with a cash dealer in a false name. Each of these offences is punishable by 2 years imprisonment but the use of SDs is considered necessary as these offences are often indicative of more serious underlying criminality including terrorist financing.

14. Offences under section 100, 100A, 101 or 101A of the *Fisheries Management Act 1991* (Cth) (the Fisheries Act) and any offence that is prescribed by the regulations are also deemed to be 'relevant offences'. These offences are included to help Australia combat the serious problem of illegal fishing in the Australian Fishing Zone.

15. An 'appropriate authorising officer' is a term used in Part 3 of the Bill with respect to emergency authorisations, and in Part 4 with respect to TD authorisations. The definition of appropriate authorising officer reflects the intrusive nature of the use of emergency authorisations and TD authorisations. Thus, an appropriate authorising officer is restricted to those that who are appropriately senior in the AFP, the ACC and a State or Territory police force.

16. A 'law enforcement agency' is defined as the AFP, the ACC or the police force of each State or Territory.

17. 'Law enforcement officer' has an expansive definition to include any AFP employee, special member or any person who is seconded to the AFP. Such an officer also includes the Commissioner and Deputy Commissioner of the AFP.

18. In relation to the ACC, a LEO means the Chief Executive Officer of the ACC or any other person who comes within the definition of 'member of the staff of the ACC' in section 4 of the Australian Crime Commission Act 2002. The definition of LEO with respect to the ACC captures all types of staff member of the ACC.

19. A LEO also includes officers of any State or Territory police force whether employed or seconded to that force.

20. A 'federal law enforcement officer' is a subset of the definition of 'law enforcement officer'. Thus, federal law enforcement officer includes all types of AFP and ACC staff members and employees including chief officer.

21. A 'State or Territory law enforcement officer' is also a subset of the definition of 'law enforcement officer', namely paragraph (c) of the definition of law enforcement officer. Such an officer means an officer employed or seconded by the police force of a State or Territory.

22. A 'tracking device authorisation' is defined as a permission given by an appropriate authorising officer under clause 39 which allows a LEO to use or retrieve a TD without a warrant.

23. 'Premises' are defined to include land, buildings and vehicles or any place whether built or not, within or beyond Australia.

24. A 'recovery order' means an order made by the Family Court under section 67U of the *Family Law Act 1975* (Cth). This Act defines a recovery order in section 67Q.

25. Subclause 6(2) provides that a LEO who is primarily responsible for executing a warrant, emergency or TD authorisation is a reference to the person named in the warrant or authorisation as such a person. Where no name appears on the warrant, the LEO primarily responsible for the warrant's execution will be the person nominated by the chief officer. Such an officer will be primarily responsible for the execution of the warrant or authorisation despite the fact that that person may not be physically present at any stage of the warrant's execution.

26. Subclause 6(3) provides that a reference to a person belonging to or who is seconded to a LEA in the case of the ACC, or a reference to a person who belongs or is seconded to the ACC, is a reference to any person who comes within the meaning of 'member of staff of the ACC' in section 4 of the ACC Act. This is to clarify that all types of ACC staff members (covered by the various paragraphs in the definition of 'staff member' in the ACC Act) are included in the reference to 'belongs or is seconded to the ACC.'

Clause 7 State offence that has a federal aspect

27. This clause defines 'State offences that have a federal aspect' for the purposes of this Bill. It will provide that a State offence has a federal aspect if the Commonwealth could have enacted a valid provision covering the State offence or the specific conduct involved in committing the State offence or, if the State offence is an

ancillary offence, then the primary offence to which that ancillary offence relates. Item 3 will also provide that a State offence has a federal aspect where the investigation of the State offence is incidental to the AFP's investigation of a Commonwealth or Territory offence.

Clause 8 External Territories

28. This clause provides that the Act is to extend to every external Territory.

Clause 9 Binding the Crown

29. This clause provides that the Act binds the Crown in right of the Commonwealth and each of the States.

30. It further provides in subclause 7(2) that nothing in the Act renders the Crown in each of its capacities liable to be prosecuted for an offence.

PART 2 – WARRANTS

Division 1 - Introduction

Clause 10 Types of warrant

31. This clause distinguishes a SD warrant from a retrieval warrant. Although the retrieval of a SD will be permitted under a SD warrant, it is also necessary to have a separate retrieval warrant which can be applied for, should the 90-day period on the authorising SD warrant expire before the device has been retrieved.

32. A SD warrant cover the four types of SDs identified in clause 6, in addition to any prescribed by regulation thereafter. A SD warrant authorises the installation, use, maintenance and retrieval of a SD.

33. Clause 10 also makes it clear that both types of warrant can be issued for more than one kind of SD. For example, a warrant may authorise the use of separate listening and tracking devices for a vehicle. It can also be issued for composite devices, that is, a device that has more than one function; for example a combined listening and tracking device. A warrant can also be issued to permit the use of more than one of the same kind of SD.

Clause 11 Who may issue warrants?

34. This clause states that a warrant under Part 2 of the Bill, that is, SD and retrieval warrants may be issued by an eligible Judge or by a nominated AAT member. In this way, the issue of SD and retrieval warrants will be subject to external scrutiny except where an emergency authorisation is given under Part 3 of Division 2 before it is approved or where an appropriate authoring officer authorises the use of an TD where the use of the device does not involve entry on to premises without permission or any interference without permission with any vehicle or thing.

Clause 12 Eligible Judges

35. This clause defines the term ‘eligible judge’ and ‘judge’. The latter has its normal meaning as a Judge of a court created by the Parliament. Eligible judges are those that consent in writing under subclause 12(2) to be nominated by the Minister under his or her power under subclause 12(3) to declare Judges, in relation to whom consents are in force, to be eligible Judges for the purposes of the Act.

36. Subclause 12(4) provides that any function or power conferred on a Judge under the Bill is conferred in a personal capacity, that is, in persona designata, and not as a court or a member of a court.

37. Subclause 12(5) provides that eligible Judges have the same protection and immunity in relation to the performance of a function or power conferred on them under the SD Act, as a Justice of the High Court has in relation to proceedings in the High Court.

Clause 13 – Nominated AAT members

38. Subclause 13(1) provides that the Minister may nominate a person who is the holder of one of the various specified appointments to the AAT. These appointments are the Deputy President, a full-time senior member, a part-time senior member or a member.

39. Subclause 13(2) provides that the Minister must not nominate a part-time senior member under subclause 13(1) unless the member is enrolled as, and has been for no less than five years, a legal practitioner of the High Court, of another federal court or of the Supreme Court of a State or the ACT.

40. Under subclause 13(3), a nomination will cease to have effect if the nominated AAT member ceases to hold their appointment under which they were nominated or the Minister withdraws the nomination in writing.

41. As with eligible judges, nominated AAT members have the same protection and immunity in the exercise of their powers under the SD Act as a Justice of the High Court has in relation to proceedings in the High Court under subclause 13(4).

Division 2 – Surveillance device warrants

Clause 14 Application for surveillance device warrant

42. This clause establishes the application process for a SD warrant. A 3-part test must be satisfied. An LEO (or a person on their behalf) apply for the issue of a SD warrant if they suspect, on reasonable grounds, that a relevant offence (or relevant offences) has been, is being, is about to be or is likely to be committed and, secondly, that an investigation into that offence (or offences) is being, will be or is likely to be conducted. The third part of the test is contained in subclause 14(1) paragraph (c) which states that the there must be reasonable grounds to believe that the use of the SD is required for the conduct of the investigation for evidence-gathering purposes in relation to the relevant offence or offences, the identity or location of the offender.

43. Subclause 14(2) provides that an application for a SD warrant for a relevant offence under subclause 14(1) by a State or Territory LEO is not permitted for a State offence with a federal aspect. In this way, State or Territory LEOs must apply for a SD warrant in relation to State or Territory offences under the relevant SD legislation in their State or Territory. Thus, an application under subclause 14(1) by a State or Territory LEO must be for a Commonwealth offence that is punishable by a maximum term of imprisonment of three years or more or for life, an offence under section 15 or 18 of the FTR Act, an offence under section 100, 100A, 101 or 101A of the Fisheries Act or an offence prescribed by regulation.

44. Subclause 14(2) requires that where a State or Territory officer is investigating a State offence, whether or not it has a Federal aspect, that officer should use State SD powers.

45. Subclause 14(3) relates to an application by an LEO for a SD warrant where a recovery order made by the Family Court for the return of a child is in force. In this situation, the LEO must suspect on reasonable grounds that a recovery order is in force and the use of a SD may assist in locating the child whose recovery is sought under the order.

46. Subclause 14(4) provides that an application for a SD warrant for a relevant offence or for the enforcement of a recovery order may be made either to an eligible judge or to a nominated AAT member.

47. Subclause 14(5) specifies what the application for a SD warrant must include. The name of the applicant and the nature, kinds and duration of the SDs sought must be included in any application. Paragraph 14(5) (b) further provides that, subject to the provision in the clause for an application to be made in the absence of an affidavit in particular circumstances, an application must be supported by an affidavit setting out the grounds on which the warrant is sought.

48. Subclause 14(6) provides that the applicant can apply for a SD without an affidavit in circumstances where a LEO believes that the immediate use of the SD is necessary in the course of the investigation for the purpose of enabling evidence to be obtained of the commission of the offence or offences, or the identity or location of the offender and it is impracticable to prepare and swear a supporting affidavit.

49. An application can also be made in the absence of an affidavit, where it is impracticable to have one prepared or sworn, for the purpose of assisting in ascertaining the location and safe recovery of a child who is the subject of a recovery order. In these circumstances, under subclause 14(7), the applicant must provide as much information as the court considers is reasonably practicable and, no later than 72 hours after the application, send a sworn affidavit to the court.

Clause 15 Remote application

50. This clause permits the application for a SD warrant to be made under clause 14 by telephone, fax, e-mail or by other means of communication where the LEO believes it is impracticable for the application to be made in person.

51. Subclause 15(2) provides that where the use of a fax is available and an affidavit has been prepared, the applicant must transmit a copy of the affidavit regardless of whether it has been sworn to the person hearing the application. By way of comparison, this procedure is consistent with existing State and Territory SD legislation. Existing Commonwealth LD legislation makes no provision for remote application. The TI Act enables application to be made by telephone or by other means of communication including fax.

Clause 16 Determining the application

52. For a SD warrant to be issued in relation to a relevant offence, the eligible Judge or nominated AAT member must be satisfied that there are reasonable grounds supporting the applicant's suspicion of the existence of three central issues set out in subclause 14(1) which form the basis of the application. That is, that a LEO suspects, on reasonable grounds, that one or more relevant offences has been, is being, is about to be or is likely to be committed and, secondly, that an investigation into that offence or offences is being, will be or is likely to be conducted. The third part of the test is contained in paragraph 14(1)(c) which states that the there must be reasonable grounds to believe that the use of the SD is required for the conduct of the investigation for evidence-gathering purposes in relation to the relevant offence(s), the identity or location of the offender

53. For applications made in relation to recovery orders issued by the Family Court, the Judge or member must be satisfied that a recovery order is in force and that reasonable grounds for the suspicion of the conditions set out in subclause 14(3), which form the basis of the application, exist.

54. For applications made remotely, the eligible judge or AAT member must also be satisfied that it was impracticable for the application to have been made in person. Similarly, subclause 16(1)(c) states that for applications made by unsworn application, the judge or member must be satisfied that it was impracticable for an affidavit to have been sworn or prepared prior to the application being made. This allows for external scrutiny of judgements made by LEOs that an application could not be made in person or that an affidavit could not be sworn in time.

55. Subclause 16(2) states that when deciding whether to issue a SD warrant, the eligible judge or AAT member must have regard to six matters. These are, the nature and gravity of the alleged offence for which the warrant is being sought, where the warrant is sought to locate and safely recover a child under a recovery order, the circumstances that led to the making of the recovery order, the extent to which the privacy of any person is likely to be affected, the existence of alternative means of obtaining the evidence or information sought to be obtained, the evidentiary or intelligence value of any information sought to be obtained and any previous warrants sought or issued under Division 2 in connection with the same offence.

56. In this way, subclause 16(2) recognises and balances the competing public interest in timely and effective law enforcement and the intrusion on the privacy of a group or individual. It is a matter for the judge or AAT member hearing the application to balance these interests in the circumstances of each application.

Clause 17 What must a surveillance device warrant contain?

57. Subclause 17(1) sets out the information a SD warrant is to contain, which includes amongst other things, the name of the applicant and the kinds of SDs authorised to be used under the warrant. This requirement ensures that LEAs have clear guidance on their powers under the SD warrant and are accountable for the proper execution of such warrants.

58. Subparagraph 17(1)(b)(xi) provides that conditions under which the SD can be used can be specified in the SD warrant. For example, where the Judge or member is satisfied in Part 5 of this Bill that the consent of an appropriate consenting official of a foreign country has been given for extraterritorial surveillance, the Judge or member can specify that the warrant authorises the use of the SD extraterritorially.

59. While the persons involved in the installation, maintenance or retrieval of the SD are not required to be named in the warrant itself (only the officer who will be primarily responsible for its execution), subparagraph 49(2)(b)(ii) of the Bill provides another accountability safeguard. It states that when reporting to the Minister after a SD warrant has ceased to be in force, the name of each person involved in the installation, maintenance or retrieval of the SD must be included in that report.

60. Subclause 17(2) provides that where the warrant authorises the use of a SD on premises, which includes a vehicle, the warrant may specify a class of vehicle. This would enable the warrant to specify all vehicles used by a suspect as a class of vehicle, thus minimising the risk of surveillance being thwarted by frequent vehicle changes. Such a reference to a class of vehicles might, for example, be ‘a vehicle to be used by a specified suspect’. This clause avoids the need to continually seek variations to warrants. However, under subparagraph 49(2)(b)(vii), any vehicles on which a SD is installed must be detailed in the report required under that clause.

61. A SD warrant must include the name and signature of the eligible judge or nominated AAT member under subclause 17(4).

62. Subclause 17(5) sets out steps that the eligible Judge or nominated AAT member must take if issuing a warrant on remote application, which include informing the applicant of the terms of the warrant and providing the original warrant to the applicant and retaining a copy for the Judge or member’s own record.

Clause 18 What a surveillance device warrant authorises

63. This clause recognises that the installation and/or retrieval of a SD may result in some interference with property, for example, in gaining entry into premises in which the SD will be used. The clause sets outs clearly what a SD warrant will authorise so as to ensure that the lawful activities and uses of SDs are known by LEOs.

64. Subclauses 18(1) paragraphs (a), (b) and (c) provide that a SD warrant authorises the use of a SD on specified premises, specified objects or class of object or on a specified person or a person whose identity is unknown, respectively.

65. Under subclause 18(2), warrants of the kind referred to in paragraphs (a), (b) and (c), will also authorise the installation, use and maintenance of a SD of the kind that is specified in the warrant on the specified premises or object or class of object or on specified or unknown persons.

66. For warrants authorising the use of a SD on specified premises, paragraph 18(2)(ii) allows entry, by force if required, onto those premises or other specified premises which adjoin or provide access to the premises for the installation, use and maintenance of the SD and for the purposes referred to in subclause 18(3).

67. For warrants which sanction the use of a SD in or on a specified object or class of objects as well as warrants used in respect of conversations, activities or for determining the location of a specified or unspecified person, subparagraphs 18(2)(b)(ii) and (c)(ii) respectively authorise the entry by force, where necessary, onto premises where the object or person (or class thereof) are reasonably likely to be. Also authorised is the entry by force, where necessary, onto other premises adjoining or proving access to those premises (not specified in the warrant) for the purposes of installing, using and maintaining the SD.

68. Subclause 18(3) lists other uses which a SD warrant authorises. These include the retrieval of a SD, the installation, use, maintenance and retrieval of any enhancement equipment, that is, equipment used to enhance a signal, image or other information obtained using the SD. The breaking open of anything for those purposes is also authorised.

69. Subclause 18(3) also allows the temporary removal of an object or vehicle from premises so a SD or enhancement equipment can be installed, maintained or retrieved. This subclause also authorises the return of the object or vehicle to those premises. Thus, if a SD malfunctions, for example, the SD warrant permits re-entry onto the premises to remove the SD to carry out repairs and to then reinstall it.

70. Paragraph 18(3) (e) authorises the connection of the SD or any enhancement equipment to a source of electricity and the use of any electricity from that source for the operation of the SD or associated enhancement equipment. The Bill does not limit what this source of electricity might be. This allows protected surveillance to occur uninterrupted by allowing for the use of SDs not run by battery.

71. Paragraphs 18(3) (f) authorises the connection of the SD or any enhancement equipment to any object or system that may be used to transmit information in any form and the use of that object or system in connection with the operation of the device or equipment. This very broad provision allows the use of any object or system, whether or not that object or system is intended or commonly used to carry information, to carry information to or from a device or equipment.

72. The highly technical nature of some SDs and the hostile nature of some premises require techniques that use existing infrastructure in order to use the SD effectively. For example, the use of existing telecommunications systems for the transmission of SD product or for the transmission of control signals to the device removes the need to install completely new systems to accomplish the same end. This means that installation time is considerably shorter, thereby exposing the installation team to less risk and reducing the probability of any compromise to the investigation.

73. In light of the highly technical nature of SDs, paragraph 18(3)(g) also permits assistance to be given by technical experts to the LEO named in the warrant for the installation, use, maintenance or retrieval of a SD or enhancement equipment.

74. In view of the covert nature of surveillance , a SD warrant will also authorise, under subclause 18(4), the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to the installation, use, maintenance or retrieval of a SD or enhancement equipment.

75. Subclause 18(5) provides a limitation on which premises can be interfered with in a SD operation. This clause states that a SD warrant can authorise the interference with the property of a person who is a third party to the investigation. However, where the interference would be on premises not named in the warrant, the Judge or member must be satisfied that it is necessary to do so in order to give effect to the warrant. This means that a LEO would not be prevented from executing a warrant on specified premises by virtue of the fact that they would first need to move property belonging to a third party.

76. In determining what conditions a warrant must be subject to, a Judge or eligible member can specify that a LEO can use a SD but not interfere with the property of a person who is not subject of the investigation in respect of which the warrant was issued even where the property adjoins or provides access to the specified premises.

77. Subclause 18(6) provides that a LEO is only to use a SD under a SD warrant if they are acting in the performance of their duty.

78. Subclause 18(7) states that nothing in clause 18 authorises the doing of anything that would require a warrant under the Telecommunications (Interception) Act 1979. Thus, a LEO must still apply for a warrant under the TI Act to do anything within the ambit of that Act as the Bill is not intended to intrude on the territory of the TI Act in any way.

Subclause 19 Extension and variation of a surveillance device warrant

79. Clause 19 allows a LEO to apply at any time while the warrant remains valid for an extension of the warrant or a variation of its terms. Such an application can be made more than once. In this way, some flexibility is built in to the warrant process so that it is responsive to the operational needs of police as and when they arise. The warrant can only be extended for a period not exceeding 90 days from the day on which it would normally expire, but for the extensions. Such an application must be made to an eligible Judge or nominated AAT member.

80. In making an application under subclause 19, a LEO is required to follow the procedures set out in clauses 14 and 15, which relate to how an application for a warrant is to be made. The LEO is also to provide the original warrant to the Judge or member hearing the application under subclause 19(2).

81. Subclause 19(4) provides that, in determining whether a SD warrant issued in relation to a relevant offence should be extended or its terms varied, the eligible Judge or nominated AAT member must be satisfied that there are reasonable grounds supporting the applicant's suspicion of the existence of three central issues set out in subclause 16(1) which form the basis of the application.

82. For applications made in relation to recovery orders issued by the Family Court, the Judge or member must be satisfied that a recovery order is in force and that reasonable grounds for the suspicion of the conditions set out in subclause 14(3), which form the basis of the application, exist.

83. For applications made remotely, the eligible judge or AAT member must be satisfied that it was impracticable for the application to have been made in person. Similarly, paragraph 16(1)(c) states that for applications made by unsworn application, the judge or member must be satisfied that it was impracticable for an affidavit to have been sworn or prepared prior to the application being made.

84. For all applications under subclause 19(4), the Judge or member when deciding the matter, must consider the six matters set out in subclause 16(2) which include the nature and gravity of the relevant offence, the extent to which the privacy of any person is likely to be affected and the likely evidentiary or intelligence value of any information sought to be obtained. If the Judge or member chooses to grant an application for extension or variation, they must endorse the new expiry date or varied term on the original SD warrant.

Clause 20 Revocation of surveillance device warrant

85. Subclause 20(1) states that an eligible Judge or nominated AAT member may revoke a SD warrant by instrument in writing at any time before it has expired. This can be done on their own initiative or by the chief officer of the appropriate LEA when they are satisfied of the matters in clause 21.

86. Subclause 21(2)(a) and (b) provide that where a SD warrant has been sought by a LEO, or by someone on their behalf, in relation to a relevant offence and the chief officer of the LEA to which the LEO belongs or is seconded, is satisfied that the use of the SD under the warrant is no longer necessary for evidence gathering purposes in relation to the commission of the relevant offence, or for determining the identity or location of the offender, then the chief officer must revoke the warrant under clause 20 and must also ensure the use of the SD authorised under the warrant is discontinued.

87. Similarly, under subclause 21(3)(a) and (b), where a SD warrant has been issued in relation to a recovery order and the chief officer of the relevant LEA believes that the use of the SD is no longer required to locate and recovery the child

under the order, the chief officer must revoke the warrant under clause and must also ensure that the use of the SD authorised by the warrant is discontinued.

88. Under subclause 20(3) the instrument revoking the warrant must be signed by the person revoking the warrant.

89. Under subclause 20(3), where an eligible Judge or nominated AAT member revokes a warrant, the Judge or member is to give a copy of the instrument of revocation to the chief officer of the LEA to which the LEO to whom the warrant was initially issued belongs or is seconded.

90. Subclause 20(5) makes it clear that if a LEO is executing the SD warrant at the time an eligible Judge or nominated AAT member revokes the warrant on their own initiative, they will not be subject to any civil or criminal liability for any act done in the proper execution of that warrant prior to the officer being made aware of the revocation. The effect is, for example, where a Judge or member has not given notice under subclause 20(3) of the revocation to the chief officer of the LEA allowing enough time for the revocation to be communicated to the relevant LEO, that officer can not be held liable for acts done that were authorised by the warrant simply because the warrant had been revoked without that revocation being brought to their attention.

Clause 21 Discontinuance of use of surveillance device under warrant

91. Clause 21 is closely related to clause 20 which relates to the revocation of SD warrants.

92. Subclause 21(1) applies where a SD warrant has been issued to a LEO. This clause creates an obligation on the chief officer of the LEA where the officer is satisfied that the grounds on which the SD warrant was issued have ceased to exist. Under subclause 21(2), where a warrant has been sought for surveillance in relation to a relevant offence, and the chief officer is satisfied that the use of the SD is no longer necessary for the purpose of enabling evidence to be obtained of the commission of the relevant offence or for determining the identity or location of the offender (for example, because the alleged offender is in custody), the chief officer is obliged to see that the use of the SD specified in the warrant is discontinued and revoke the warrant under clause 20.

93. Similarly, subclause 21(3) provides that where the SD warrant was sought to give effect to a recovery order issued by the Family Court for the return of a child and the use of a SD is no longer required for the purpose of locating and safely recovering the child who is the subject of the order (for example, because the child has been recovered), the chief officer must take the same steps as above.

94. Subclause 21(4) provides that if the chief officer is notified that the warrant has been revoked under section 20, they are to see that the use of the SD authorised by the warrant is discontinued as soon as practicable.

95. Subclause 21(5) paragraphs (a) and (b) provide that where the LEO to whom the warrant was issued or who is named in the warrant as being the officer primary

responsible for its execution is satisfied that the SD is no longer required for the purpose for which it was issued, they must immediately inform the chief officer of their LEA. The chief officer, under subclause 21(2) or (3) – whichever is relevant in the circumstances – must take the necessary steps to see that the use of the SD is discontinued and revoke the warrant under clause 20. In this way, it is intended that SDs are used only when required for the purpose for which they were issued.

Division 3 – Retrieval warrants

Clause 22 Application for retrieval warrant

96. Where a SD has expired before a LEO has been able to remove the device that was lawfully installed, clause 22 allows the LEO to apply to an eligible Judge or nominated AAT member for a warrant to retrieve the SD, however such an application is not mandatory. This means, for example, that where retrieving the SD presents a disproportional cost to the LEA or some danger to the retrieval team, the SD can remain in place but cannot be used.

97. Under subclause 22(1), the LEO must suspect on reasonable grounds (set out in an affidavit in support of the application) that the SD that was lawfully installed on premises or in or on an object is located on those or other premises or object, before a retrieval warrant can be sought.

98. Subclause 22(4) makes provision for an unsworn application to be made where the retrieval of the SD is necessary and it is impracticable for an affidavit to be prepared or sworn before the application for the warrant is made. As with other unsworn applications for warrants under the Bill, the applicant must provide the Judge or member with as much information as they consider is reasonably practicable in the circumstances and within 72 hours of making the application, send a duly sworn affidavit to the Judge or member who decided the application as per subclause 22(5).

Clause 23 Remote application

99. Provision is made for an application for a retrieval warrant to be made remotely where the LEO believes it is impracticable for such an application to be made in person. An application under clause 22 can be made by telephone, fax, e-mail or any other means of communication.

100. Under subclause 23(2), where transmission by fax is available and an affidavit has been prepared, whether sworn or unsworn, the applicant must transmit a copy of the affidavit to the Judge or member who will be determining the application.

Clause 24 Determining the application

101. In deciding whether to issue a retrieval warrant, the eligible Judge or nominated AAT member must have regard to several things. The Judge or member must be satisfied that there are reasonable grounds for the LEO's suspicion that the SD is still on the premises or in or on the object to which it was installed, or on other premises or in or on another object.

102. Where the application is made in the absence of an affidavit, the Judge or member must be satisfied that it would have been impracticable for an affidavit to be or prepared before the application was made.

103. Where the application was made remotely, the Judge or member must be further satisfied that it would have been impracticable for the application to have been made in person.

104. Subclause 24(2) provides for further considerations that the Judge or member must have regard to when deciding whether or not to issue a retrieval warrant. These considerations seek to balance the competing public interests of a right to privacy and the effective enforcement of the law. Thus, the Judge or member must consider the extent to which the privacy of any person is likely to be affected and the public interest in retrieving the SD. The latter refers to cost considerations and the risk that law enforcement methodologies and investigations may be compromised should the SD be located.

Clause 25 What must a retrieval warrant contain?

105. The retrieval warrant must contain several matters as specified in clause 25. The first of these is that the person hearing the application is satisfied that there are reasonable grounds founding the suspicion on which the application is based and, for unsworn applications or those made remotely, that it was impracticable for an affidavit to be prepared or sworn and for the application to be made in person, as per paragraph 25(1)(a).

106. The Judge or member must also have turned their mind to the privacy and public interest considerations set out in subclause 24(2).

107. The warrant must be signed by the person issuing it and include their name and must specify the same matters required to be specified in a SD warrant insofar as they relate to a retrieval warrant. These are the premises or object from which the warrant is to be retrieved, the period during which the retrieval warrant is in force (no more than 90 days), the conditions subject to which premises may be entered, the name of the LEO primarily responsible for the warrant's execution, the name of the applicant, the date the warrant is issued and the types of SD authorised to be retrieved under the warrant.

108. Subclause 25(3) provides that after issuing a warrant on the basis of a remote application, the Judge or member must inform the applicant of its terms, the date and time when the warrant was issued and give the warrant to the applicant as soon as practicable. The Judge or member must retain a copy of the warrant for their own record.

Clause 26 What a retrieval warrant authorises

109. The execution of a retrieval warrant is subject to any conditions that the eligible Judge or nominated AAT member imposes on the warrant under subparagraph 25(1)(b)(vii).

110. The warrant authorises, subject to those conditions, the retrieval of the SD which is named in the warrant and any enhancement equipment used in conjunction with the device.

111. A retrieval warrant also authorises the entry, by force where necessary, onto premises where the LEO believes the SD to be located and onto other premises adjoining or providing access to those premises for the purposes of retrieving the device and enhancement equipment.

112. A warrant will also authorise the breaking open of any thing as long as it is for the purpose of retrieving the SD or enhancement equipment.

113. Where the device or equipment has been installed on or in an object or vehicle, the warrant will authorise the removal of that object or vehicle from any place so that the device or equipment can be removed. The object must then be returned to that place.

114. Also authorised under subclause 26(1) is the provision of technical assistance to the LEO named in the warrant for the retrieval of the device or equipment.

115. Special provision is made under subclause 26(2) for the retrieval of a TD. This allows the use of the device and any enhancement equipment for the sole purpose of locating the device so that it, and any enhancement equipment, may be located and then retrieved.

116. Subclause 26(3) permits the doing of anything required to conceal that anything has been done in relation to the retrieval of the SD or enhancement equipment under the warrant. However, the retrieval warrant cannot authorise the use, except as allowed in subclause 26(2), of the SD specified in the warrant.

Clause 27 Revocation of retrieval warrant

117. Clause 27 allows a retrieval warrant to be revoked by an eligible Judge or nominated AAT member by instrument in writing at any time before it expires, according to the period of validity specified in the warrant. A Judge or member can do so on his or her own initiative under subclause 27(1).

118. Subclause 27(2) also provides that the chief officer of the LEA to which the LEO to whom the warrant was issued belongs or is seconded, must revoke a retrieval warrant, in writing, if they are satisfied that the grounds for the issue or the warrant no longer exist.

119. Under subclause 27(3), the instrument that revokes the warrant must be signed by the Judge or member or the chief officer of the LEA, as the case requires.

120. Under subclause 27(4), if a Judge or member revokes a warrant, they are to give a copy of the instrument of revocation to the chief officer of the LEA to which the LEO to whom the warrant was issued belongs or is seconded.

121. Under subclause 27(5), if the LEO who was issued the warrant or who is named as the person primarily responsible for its execution believes that the grounds for the issue of the warrant no longer exist, they must inform the chief officer of their LEA immediately. The chief officer, under subclause 27(2), must then, if they are satisfied that the grounds on which the warrant was issued no longer exist, revoke the warrant.

PART 3 – EMERGENCY AUTHORISATIONS

Clause 28 Emergency authorisation – serious risks to person or property

122. Clauses 28, 29 and 30 provide for the use of a SD without a warrant in certain emergency situations where it is not practicable to obtain a warrant from an eligible Judge or nominated AAT member. Clauses 28, 29 and 30 set out the procedure for the issue of an emergency authorisation (an authorisation) in three distinct cases where the circumstances justify the use of a SD without prior judge or AAT member authorisation.

123. Where a LEO reasonably suspects that an imminent threat of serious violence to a person or substantial damage to property exists, clause 28 allows the LEO to apply to an appropriate authorising officer (for example, the Commissioner of the AFP or the relevant State or Territory police force, or the Chief Executive Officer of the ACC) for an authorisation for the use of a SD in the course of an investigation of a relevant offence where such a threat exists. The LEO must also reasonably suspect that the use of the SD is immediately necessary for the purpose of responding to the threat of serious violence to a person or substantial damage to property. The LEO must also suspect that the circumstances are so serious and the matter of such urgency that the use of the SD is warranted. Thus, clause 28 will allow LEAs to respond quickly and effectively to the activities of terrorists.

124. Finally, the LEO must suspect that it is not practicable in the circumstances to apply to an eligible Judge or nominated AAT member for a SD warrant. Clause 28 thus establishes a high threshold, characterised by urgency, immediacy and seriousness, for an emergency authorisation to be issued.

125. Under subclause 28(2), a police officer of a State or Territory cannot apply for an emergency authorisation for State offences with a federal aspect as such offences are not to be included as a ‘relevant offence’ for the purposes of clause 28. Thus, it is only Commonwealth offences that can be used as a basis for an authorisation under clause 28 in the State context

126. Under subclause 28(3), such an application may be made orally, in writing, by telephone, email or fax or any other means of communication.

127. Subclause 28(4) provides that if the appropriate authorising officer is satisfied that there are reasonable grounds for the LEO's suspicion of the grounds which found the application, that is, the grounds in subclause 28(1), the authorising officer may give an emergency authorisation.

Clause 29 Emergency authorisation – urgent circumstances relating to recovery order

128. The second circumstance in which a LEO can apply for, and where an appropriate authorising officer can give, an emergency authorisation is where a recovery order is in force and the LEO reasonably suspects that the circumstances are so urgent as to warrant the immediate use of a SD to give effect to the recovery order. It must also be impracticable in the circumstances to apply for a SD warrant.

129. To issue an emergency authorisation, the appropriate authorising officer must be satisfied that there are reasonable grounds supporting the LEO's suspicion of the existence of the grounds in paragraph 29(1(b) .

130. Under subclause 29(2), an application under this section can be made orally, in writing, by telephone, fax or email or any other means of communication.

Clause 30 Emergency authorisation – risk of loss of evidence

131. The third situation in which an LEO can apply for an emergency authorisation is in the conduct of an investigation for offences specified in subclause 30(1) (Commonwealth serious drug, terrorism, treason, aggravated people trafficking and espionage offences) where the LEO reasonably suspects that the use of the SD is immediately necessary to prevent the loss of any evidence relevant to an investigation of the specified offence.

132. Special provision is made for these particular offences because of their importance to the Commonwealth and/or the difficulty of obtaining evidence by other means.

133. The LEO must suspect that the circumstances are so serious and urgent as to warrant the use of a SD without court authorisation and that it is not practicable to apply for a SD warrant in the normal manner.

134. As with authorisations under clauses 28 and 29, an application can me made orally, in writing, by telephone, fax or email or any other means of communication.

135. An appropriate authorising officer may give an emergency authorisation in relation to the conduct of an investigation into a specified offence where they are satisfied that an investigation is indeed being conducted into one of the specified offences and there are reasonable grounds for the LEO's suspicion that a SD is necessary to prevent the loss of relevant evidence, that the matter is both serious and urgent and that applying for a SD warrant in the normal manner is not practicable.

Clause 31 Record of emergency authorisation to be made

136. Clause 31 requires the appropriate authorising officer, having issued an emergency authorisation, to make a written record of giving that authorisation. The record is to include the name of the applicant, the date and time the authorisation was given and the nature of the authorisation. This record is later to accompany the application for approval by an eligible Judge or nominated AAT member under clause 33.

Clause 32 Attributes of emergency authorisations

137. Clause 32(1) provides that an emergency authorisation given under clauses 28, 29 or 30 may authorise the LEO to whom it is given to use multiple SDs of the same or of different types.

138. Subclause 32(2) states that authorisations given under clauses 28, 29 or 30 permit the LEO to whom it was issued to do anything that a SD warrant may authorise the LEO to do (as set out in clause 18).

139. Under subclause 32(3), a LEO may only use a SD authorised under an authorisation if he or she is acting in the performance of his or her duty.

140. Subclause 32(4) provides that clause 32 is not intended to authorise the doing of anything for which a warrant under the Telecommunications (Interception) Act 1979 would be required.

Clause 33 Application for approval of emergency authorisation

141. Where a device has been used for surveillance under an emergency authorisation given by an appropriate authorising officer, approval of that use must subsequently be sought from an eligible Judge or nominated AAT member within 2 business days from when the authorisation was given. A ‘business day’ is defined in clause 6.

142. Under subclause 33(2), an application for approval must include the name of the applicant seeking approval, the kind or kinds of SD sought to be approved and must be supported by an affidavit which sets out the grounds on which the approval is sought. A copy of the written record of the emergency authorisation made under clause 31 must also be included with the application.

143. If a SD warrant is sought, the nature and the duration of the warrant must also be included on the application under subparagraph 33(2)(a)(ii). Under subclause 35(4) the Judge or member is empowered to issue a SD warrant for the continued use or may order cessation of use of the SD.

144. Under subclause 33(3), the Judge or member can refuse to consider the application for approval until the applicant provides the Judge or member with all the information they require in a form specified by the Judge or member.

Clause 34 Consideration of application

145. When deciding whether to approve an emergency authorisation issued by an appropriate authorising officer, an eligible Judge or nominated AAT member must take into account numerous considerations, including the intrusive nature of SD use.

146. The considerations are listed in subclause 34(1) for authorisations given under clause 28, which relates to authorisations given where there is a belief that serious risk to person or property exists. The Judge or member must consider the nature of the risk of serious violence to a person or substantial damage to property which the LEO suspected at the time of applying for the authorisation. The Judge or member must also consider the extent to which issuing a SD warrant would have helped reduce or avoid the risk to person or property.

147. The extent to which LEOs could have used alternative methods to help reduce or avoid the risk to a person or property must also be considered, balanced with how much the use of these alternative methods of investigation would have helped reduce or avoid the risk. The Judge or member must also consider how much the use of such methods would have prejudiced the safety of the person or property because of delay or for another reason.

148. The Judge or member must also consider whether, in the circumstances, it was indeed practicable for the LEO to apply for a SD warrant in the normal manner or whether the urgency and seriousness of the risk justified the use of an emergency authorisation.

149. Subclause 34(2) relates to emergency authorisations issued for use in urgent circumstances relating to a recovery order under clause 29. The eligible Judge or nominated AAT member once again must turn their mind to the intrusive nature of SD use while considering the urgency of the need to enforce the recovery order. The Judge or member must also consider the extent to which the use of a SD device would assist in the location and recovery of the child under the recovery order. The extent to which the LEO could have made use of alternative methods to assist in the location and safe recovery of the child who is the subject of the recovery order must also be taken into account in the decision of whether or not to approve the emergency authorisation.

150. The Judge or member must also look at how much the use of alternative methods to the use of a SD would have prejudiced the effective enforcement of the recovery order and whether or not it was practicable, in the circumstances, to apply for a SD warrant with or without a sworn supporting affidavit, in person or by remote application.

151. In considering these factors, the Judge or member stands in the shoes of the appropriate authorising officer at the time they made the decision to issue the emergency authorisation in light of the information that was available to them at the time of that decision. In this way, the Judge or member determines whether the use of the SD without court approval was justified at the time, given the information that was before the appropriate authorising officer.

152. Subclause 34(3) provides that when deciding whether to approve an emergency authorisation issued under section 30, which deals with the risk of loss of evidence for specified Commonwealth serious drug, terrorism, treason, aggravated people trafficking and espionage offences, the eligible Judge or nominated AAT member must consider the nature of the risk of loss of evidence and the extent to which using the SD may have helped reduce the risk. The possible use of alternative methods of investigation by LEOs to achieve their purpose must be considered in light of the intrusive nature of using a SD. This is to be balanced with how much the use of alternative methods could have helped reduce or avoid the risk. The Judge or member must also be satisfied that it was not practicable for a SD warrant to be applied for at the time.

Clause 35 Judge or nominated AAT member may approve giving of emergency authorisation

153. This clause sets out what an eligible Judge or nominated AAT member must be satisfied of in order to approve an emergency authorisation.

154. For authorisations issued in circumstances where the appropriate authorising officer is satisfied of the grounds under subsection 28(1), including that an imminent threat of serious violence to a person or substantial damage to property exists, the Judge or member may approve the use of the SD under the authorisation if they are satisfied that there were reasonable grounds to suspect that such a risk did indeed exist at the time the authorisation was given.

155. The Judge or member must also be satisfied that there were reasonable grounds to suspect that using a SD may have helped reduce the risk of violence to a person or damage to property from occurring and that it was not practicable in the circumstances for an application to be made for a SD.

156. Subclause 35(2) relates to the issue of an emergency authorisation under section 29, that is, for the purposes of enforcing a recovery order in urgent circumstances An eligible Judge or nominated AAT member may approve the use of the SD under an authorisation if satisfied that there was a recovery order in force ay the time the authorisation was given, that reasonable grounds existed supporting the suspicion that the enforcement of the recovery order was urgent and that the use of a SD may have assisted in the prompt location and safe recovery of the child. The Judge or member must also be satisfied that it was not practicable in the circumstances for an LEO to apply for a SD warrant.

157. Subclause 35(3) sets out the matters that an eligible Judge or nominated AAT member hearing the application for approval of an emergency authorisation must be satisfied of for an authorisation issued under clause 30, that is, where there was a risk of loss of evidence for the specified Commonwealth offences.

158. The Judge or member may approve the application if they are satisfied that a risk of a loss of evidence existed at the time the emergency authorisation was given and that using a SD may have helped reduce that risk. As with all emergency authorisations, the Judge or member must also be satisfied that an application for a

SD warrant was not practicable in the circumstances as they existed at the time the authorisation was applied for.

159. Subclause 35(4) sets out the options available to an eligible Judge or nominated AAT member when they have approved the giving of an emergency authorisation. Under paragraph 35(4)(a) the Judge or member may issue a SD warrant for the continued use of the SD as if the application for the emergency authorisation were in fact an application for a SD warrant under Division 2 of Part 2 of the Bill, providing that the activity that required surveillance continues to exist. In this way, the duration of the warrant is then subject to the 90 day limit and the Judge or member is empowered to impose conditions or restrictions on the warrant, for example, conditions upon which premises may be entered to maintain a SD.

160. Paragraph 35(4)(b) provides that where the Judge or member is satisfied that since the application for the authorisation was made, the activity which required surveillance has ceased, they can make an order that the use of the SD cease.

161. Subclause 35(5) sets out the options where the eligible Judge or nominated AAT member chooses *not* to approve the giving of an emergency authorisation under clauses 28, 29 and 30 at subclauses 35(1),(2) and (3) respectively. In these circumstances, the Judge or member may order that the use of the SD cease altogether. However, where the Judge or member believes that the situation did not warrant an emergency authorisation at the time it was issued but that the use of a SD under Division 2 of Part 2 has now become necessary, they may issue a SD warrant for the future use of such a device. In this case, the application for the approval of the emergency authorisation shall be treated as if it was an application for a SD warrant under Division 2 of Part 2.

162. Subclause 35(6) provides that, in any case, the eligible Judge or nominated AAT member may order that any information obtained from or relating to the exercise of powers under an emergency authorisation or any record of that information be dealt with in manner specified in the order. The Judge or member may not order that such information be destroyed because such information, while improperly obtained, may still be required for a permitted purpose in 45(5), such as an investigation into the improper surveillance. Division 5 of the Bill governs what can be done with such information.

Clause 36 Admissibility of evidence

163. This clause provides that evidence obtained under an emergency authorisation which has subsequently been approved by an eligible Judge or nominated AAT member will be admissible in any proceedings. Thus, the fact that the evidence was obtained under an authorisation prior to receiving approval does not render such evidence inadmissible.

PART 4 – USE OF CERTAIN SURVEILLANCE DEVICES WITHOUT WARRANT

Clause 37 Use of optical surveillance devices without warrant in certain circumstances

164. Subclause 37(1) provides that where the use of an OSD will not involve entry onto premises without permission or interference without permission with any vehicle or thing, a LEO (not including a police officer of a State or Territory police force) may, without a warrant, use such a device in the course of their duties. The corollary of this is that where the use of the OSD will result in a entry onto premises or interference with any vehicle or thing without permission, a LEO within the meaning of paragraph (a) or (b) of the definition of LEO in subclause 6(1), must make an application for a SD warrant in the normal manner (or in certain limited circumstances, for a tracking device authorisation under clause 39).

165. The functions set out in section 8 of the AFP Act and those in section 7A of the ACC Act are functions that are within the course of the duties of federal LEOs.

166. Subclause 37(1) makes clear that it is to take precedence over any law of the Commonwealth or of a State or Territory, including common law principles, which forbids the use of OSDs without a warrant. However, the existence of this power does not impliedly prohibit this activity for person who is not covered by this power.

167. Subclause 37(2) provides that LEOs of State or Territory police acting in the course of their duties can use an OSD without a warrant in the investigation of a relevant offence (as defined in clause 6), excluding a State offence with a federal aspect (where their powers of their own jurisdiction would need to be used), if the use of the OSD does not involve entry onto premises without permission or interference without permission with any vehicle or thing. Under subclause 37(3), State and Territory LEOs can also use an OSD without a warrant under these conditions for determining the location and effecting the safe recovery of a child under a recovery order. This is so despite any other law of the Commonwealth, State or Territory, including any principles of common law, which forbids the use of OSDs without a warrant.

168. The implication of clause 37 is that LEOs of State or Territory police forces remain subject to the relevant laws regarding the use of OSDs in their State or Territory for all State or Territory offences. Thus, such officers are not empowered to use OSDs without a warrant by virtue of subclause 37(1) for State offences with a federal aspect.

Clause 38 Use of surveillance devices without warrant for the listening to or recording of words in limited circumstances

169. Subclause 38(1) permits a Federal LEO acting in the performance of their duties to use a SD for any purpose involving listening to or recording words spoken without a SD warrant. However, the ability of an AFP or ACC employee (including those seconded to the agency) to carry out this surveillance is limited to the functions

of officers, employees or staff members of either agency as set out in the AFP and ACC Acts respectively.

170. Paragraph 38(1)(c) further provides that the use of the device for the listening or recording of spoken words is confined to circumstances where the LEO is the speaker of the words or where the person to whom the LEO is speaking, intends or should reasonably expect the words to be heard by the LEO or class or group of such persons including the LEO. So, for example, where an undercover LEO who is wearing a listening device speaks to a person about their suspected involvement in criminal activities, a device to record the conversation can be used without the LEO having to apply for a warrant to do so.

171. Subclause 38(2) also allows State or Territory LEOs to use a SD for any purpose relating to listening to or recording words spoken by a person in circumstances similar to subclause 38(1). However, the LEO must be acting in the course of their duties in either the investigation of a relevant offence (not including a State offence that has a federal aspect as per the definition in clause 7) or in relation to the location and safe recovery of a child under a recovery order.

172. Paragraphs (a) and (b) of subclause 38(2) and 38 (3) provide further limitations on the use of a SD for listening and recording purposes in the investigation of a relevant offence or for the enforcement of a recovery order, respectively. As with federal LEOs, such use is to be confined to circumstances where the State or Territory LEO is the speaker of the words or where the person to whom the LEO is speaking, intends or should reasonably expect the words to be heard by the LEO or class or group of such persons including the LEO.

173. Alternatively, a State or Territory LEO can listen to or record the words with the express or implied consent of a person who comes within paragraph 38(2)(a).

Clause 39 Use and retrieval of tracking devices without warrant in certain circumstances

174. Clause 39 allows limited use of a tracking device with internal police authorisation only. This is in reflection of the less intrusive nature of TDs as compared with other types of SD. However, where such use requires a greater level of intrusion (such as entry onto premises without permission) a full SD warrant would be required.

175. Subclause 39(1) provides that a LEO may apply to an appropriate authorising officer to use a TD without a warrant in the investigation of a relevant offence provided that the installation or retrieval of a TD does not involve entry onto premises without permission or an interference with the interior of a vehicle without permission as per subclause 39(37). Thus, under a TD authorisation, a LEO could put a TD on the chassis of a vehicle but could not put such a device under a seat in the vehicle, even if a vehicle door was unlocked.

176. The authorising officer must give their permission in writing. Subclause 39(4) stipulates that subclause 39(1) it is to take precedence over any other law of Australia,

including any principles of common law, which forbids the use of a TD without a warrant.

177. Subclause 39(2) provides that LEOs of State or Territory police forces remain subject to the relevant laws regarding the use of TDs in their State or Territory for all State or Territory offences. Thus, such officers are not empowered to use TDs without a warrant by virtue of subclause 39(1) for State offences that have a federal aspect. For such use, State and Territory officers would be need to use the powers of their own jurisdiction.

178. Subclause 39(3) authorises a LEO to use a TD without a warrant, with the written permission of an appropriate authorising officer, to locate and recover a child in respect of whom a recovery order has been made, provided that the installation or retrieval of the TD does not involve a entry into premises without permission or an interference with the interior of a vehicle without permission (subclause 39(7)). As with subclause 39(1), subclause 39(4) stipulates that subclause 39(3) is also to take precedence over any other law of Australia, including any principles of common law, which forbids the use of a TD without a warrant.

179. Subclause 39(5) provides that where an appropriate authorising officer has given their written permission for the use of a TD for the investigation of a relevant offence or for the enforcement of a recovery order, the permission may authorise the LEO to use more than one TD.

180. Subclause 39(6) states that if an appropriate authorising officer has given their permission under subclause 39(1) or (3) for the use of a TD without a warrant, they may also authorise the retrieval of such a device without a warrant.

181. Subclause 39(8) sets out the application process for obtaining the permission of an appropriate authorising officer for the use of a TD under subclauses 39(1) or (3). A LEO can make such an application to an appropriate authorising officer orally or in writing and is required to address the matters that the LEO would be required to address if they were making an application for a SD warrant, for example, that a relevant offence has been, is being, is about to be or likely to be committed and that the use of the SD is necessary to obtain evidence of the commission of the offence.

182. Subclauses 39(9) and (10) apply specified parts of clauses 18 and 26 of the Bill to TD authorisations issued under clause 39.

183. Subclause 39(9) provides that various parts of clause 18 are to apply to a TD authorisation as if reference in those provisions to a ‘SD warrant’ and to a ‘surveillance device’ were references to a ‘TD authorisation’ authorising the use of a TD and a ‘tracking deceive’ respectively. Thus, a TD authorisation may authorise the use of a TD in or on a specified object or class thereof, the installation, use and maintenance of a TD or enhancement equipment in or on a specified object or class thereof and the provision of assistance or technical expertise to the LEO named in the authorisation for those purposes. The authorisation also permits the retrieval of the TD.

184. The TD authorisation also permits the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to the installation, use, maintenance or retrieval of the TD or enhancement equipment under the authorisation.

185. Subclause 39(10) imports a number of requirements from warrant provisions in this Bill. For the purposes of clause 39, references to these terms 'retrieval warrants' and 'surveillance devices' are to be taken as if they were references to a 'tracking device authorisation' and a 'tracking device' respectively. Thus, the TD authorisation will authorise the retrieval of the TD and enhancement equipment and the breaking open of any thing for this purpose, amongst other things permitted in those parts of clause 26 specified in subclause 39(10).

186. Subclause 39(11) permits a LEO to use a TD only if they are to use it in the performance of his or her duties.

Clause 40 Record of tracking device authorisations to be kept

187. The appropriate authorising officer who has given their permission for the use of a TD without a warrant under clause 39 must make a written record of giving the authorisation as soon as practicable after giving the authorisation. The record is to contain the matters listed in paragraphs (a) to (k), which include the name of the applicant for the authorisation, the date and time when permission was given, the nature of the authorisation given and the period during which the warrant is in force, not exceeding a period of 90 days. It is also to include whether the warrant relates to an alleged relevant offence or to a recovery order and any conditions under which a TD is to be used.

PART 5 – EXTRATERRITORIAL OPERATION OF WARRANTS

Clause 41 Definitions

188. Clause 41 provides for definitions for the purposes of Part 5.

189. An 'appropriate consenting official' is defined as an official of a foreign country with authority in that country to give consent to the extraterritorial use of SDs in that country or on a vessel or aircraft registered under the laws of that foreign country.

190. Both 'contiguous zone' and 'territorial sea' are to have the same meaning as in the *Seas and Submerged Lands Act 1973* (Cth).

191. The 'Australian fishing zone' is to have the same meaning as the term does in the Fisheries Act.

Clause 42 Extraterritorial operation of warrants

192. Clause 42 relates to surveillance required in a foreign country or on a vessel or aircraft which is registered under the law of a foreign country and is in or above

waters beyond the outer limit of Australian territorial waters (extraterritorial surveillance). Such surveillance requires the permission of the foreign country. Such permission is not necessary for an Australian flagged vessel in international waters nor for a vessel or aircraft of a foreign country that is in Australia or in or above waters within the outer limits of the territorial sea of Australia as per subclause 42(8).

193. Clause 42 is only to apply to LEOs referred to in paragraphs (a) and (b) of the definition in subclause 6(1). Therefore, State and Territory officers may not engage in extra-territorial surveillance as permitted by this Bill.

194. The clause covers two distinct situations; the first is where a SD warrant is already in existence and it has become apparent to the federal LEO that surveillance is required extraterritorially and the permission of the foreign State has not yet been obtained (subclause 42(3)). The second situation is where a warrant is yet to be issued or the use of an emergency authorisation is yet to be approved, and the need for extraterritorial surveillance becomes known to the federal LEO. These are dealt with by subclauses 42(1) and 42 (2) respectively.

195. Subclause 42(1) provides that before a warrant for the investigation of a relevant offence has been applied for by a federal LEO and it has become apparent to the applicant that there will be a need for extraterritorial surveillance for the purposes of that investigation, the eligible Judge or nominated AAT member considering the application for the SD warrant must not permit the warrant to authorise that surveillance unless they are satisfied that it has been agreed to by a appropriate consenting official of the foreign country.

196. Subclause 42(2) covers the situation where an application has been made for the approval of the use of a SD under an emergency authorisation given by an appropriate authorising officer who is a federal LEO and where the consideration of the application has not been finalised, and it has become apparent to the applicant that there will be a need for extraterritorial surveillance to assist in the investigation. In these circumstances, the eligible Judge or nominated AAT member is not to authorise the extraterritorial surveillance under the warrant unless they are satisfied that the surveillance has been agreed to by an appropriate consenting official of the foreign country.

197. Subclause 42(3) provides that if a warrant has already been issued for the investigation of a relevant offence by a federal LEO, and following the issue of the warrant it becomes apparent to the LEO who is primarily responsible for executing the warrant that there will be a need for extraterritorial surveillance to assist in that investigation, the warrant is taken to permit that surveillance only if it has been agreed to by a appropriate consenting official of the foreign country. In this way, extraterritorial surveillance is carried out under an Australian warrant, with the agreement of the foreign State, which ensures that such surveillance is subject to appropriate accountability and probity measures under domestic law.

198. Subclause 42(4) states that where a foreign vessel is in waters beyond the outer limits of the territorial sea of Australia but is within the outer limits of the contiguous zone of Australia, the agreement of an appropriate consenting official of the foreign country, the laws of which the vessel of aircraft is registered under, is not

required for the conduct of surveillance while the vessel is in this zone for particular offences. The offences are those relating to the customs, fiscal, immigration or sanitary laws of Australia. This is despite subclauses (1), (2) and (3) of clause 42. Such offences would include but not be limited to, offences against: the *Migration Act 1958* and the Customs Act. Any relevant offence in any Act which conforms to the description: customs, fiscal, immigration or sanitary laws' would be an offence that would permit surveillance under this subclause.

199. 42(5) provides that where a vessel that is registered under the law of a foreign country is in waters beyond the outer limits of the territorial sea of Australia but not beyond the outer limits of the Australia fishing zone, there is no requirement for the agreement of an appropriate consenting official of the foreign country where surveillance is required for offences against section 100, 100A, 101 or 101A of the Fisheries Act which deal with illegal fishing. This is despite subclauses (1), (2) and (3) of clause 42.

200. Subclause 42(6) states that the chief officer of the LEA to which the LEO who applied for the warrant belongs or is seconded, must give the AG written evidence that the surveillance has been agreed to by a appropriate consenting official of the foreign country. The chief officer is to provide this evidence of consent as soon as practicable after the surveillance has commenced under a warrant in a foreign country or on a foreign vessel or aircraft where such consent is required.

201. Subclause 42(7) covers the circumstance where surveillance will need to be carried out on a vessel or aircraft that is registered under the laws of a sovereign country and is located in or above the territorial waters of a different foreign country. In this case, the reference to obtaining the agreement of an 'appropriate consenting official of the foreign country' is taken to mean such a representative of *each* foreign country concerned. For example, if a SD is to be used on a vessel of flag State A and the vessel enters the territorial waters of State B, agreement of an appropriate consenting official from both State A and State B would be required.

Clause 43 Evidence obtained from extraterritorial surveillance inadmissible unless court satisfied properly obtained

202. This clause provides that evidence that has been obtained under subclauses 42 (1),(2) or (3) cannot be tendered in proceedings relating to the relevant offence for which the surveillance was carried out, unless the court is satisfied that the surveillance was agreed to by a appropriate consenting official of the foreign country.

PART 6 – COMPLIANCE AND MONITORING

Division 1 Restrictions on use, communication and publication of information

Clause 44 What is protected information?

203. Clause 44 defines 'protected information' for the purposes of Division 1 of Part 5.

204. ‘Protected information’ is information subject to restrictions on its use, communication or publication because such information relates to law enforcement operational matters and because the use of such information may harm the privacy of individuals or groups.

205. Clause 44 contains broadly different types of protected information, which may overlap, at paragraphs (a) to (d).

206. Paragraph (a) of subclause 44(1) includes information, including records and transcripts that are obtained from the use of a SD under a warrant, an emergency authorisation or a TD authorisation.

207. Paragraph (b) of subclause 44(1) includes any information relating to (i) an application for, issue of, existence of or expiry of a warrant, an emergency authorisation or a TD authorisation; or (ii) an application for approval of powers exercised under an emergency authorisation.

208. Paragraph (c) of subclause 44(1) includes any information beyond that included in paragraphs (a), (b) which is likely to enable the identification of a person, object or premises specified in a warrant, an emergency authorisation or a TD authorisation.

209. Paragraph (d) of subclause 44(1) includes any other information obtained by a LEO either without the authority of a warrant or a TD authorisation; or without the authority of an emergency authorisation that was subsequently approved; in contravention of a requirement to obtain such a warrant, TD authorisation or emergency authorisation. Such information may overlap with other types of protected information but is to be distinguished on the grounds that paragraph (d) information has, in some sense, been improperly or illegally obtained and is subject to more fewer exceptions allowing its subsequent use or communication.

210. Subclause 44(2) clarifies that protected information obtained under an emergency authorisation before that emergency authorisation has been approved by an eligible Judge or nominated AAT member, provided that such an authorisation is not in contravention of the requirement to be reviewed under clause 33, falls under paragraph (a) of the definition of ‘protected information’ rather than paragraph (e). This is because such information has not been improperly or illegally obtained and thus may be used, communicated or published subject to the exceptions in clause 45 which relate to paragraph (a) material rather than the more limited set of exceptions which apply to paragraph (d) material.

Clause 45 Prohibition on use, recording, communication or publication of protected information or its admission in evidence

211. Clause 45 creates two offences with respect to the unlawful use, recording, communication, publication or admission in evidence of protected information.

212. Subclause 45(1) makes it an offence if a person uses, records, communicates or publishes any information, or admits it in evidence, when that information falls

within the definition of protected information and such use is not permitted by one of the exceptions in this section. The maximum penalty is 2 years imprisonment.

213. Example: if a LEO, in possession of a record of surveillance conducted under a SD warrant, provides a copy of that record to an associate for a purpose other than those provided for in subclauses 45(5) and (5) (such as to assist with the investigation of a minor offence which does not fall within the definition of 'relevant offence'), that LEO would be guilty of an offence.

214. Subclause 45(2) makes it an offence if a person uses, records, communicates or publishes any information, or admits it in evidence, when that information falls within the definition of protected information and such use is not permitted by one of the exceptions in this section, and furthermore, such use is subject to one of the aggravating factors set out in paragraph 45(2)(d). The maximum penalty is 10 years imprisonment. A higher penalty is applicable with respect to this offence because it is an aggravated offence.

215. Example: if a LEO, in possession of a record of surveillance conducted under a SD warrant, provides a copy of that record to an associate for a purpose other than those provided for in subclauses 45(3) and (4) (such as to assist with the investigation of a minor offence which does not fall within the definition of 'relevant offence'), and the provision of that copy results in danger to a person, that LEO could be guilty of an offence.

216. Subclause 45(3) provides that, subject to the exceptions in subclauses 45(5) and (5), protected information may not be admitted in evidence in any proceedings. This provision should be read in conjunction with subclause 4(2).

217. Subclause 45(5) provides for a set of circumstances, not directly related to law enforcement, for which protected information may be lawfully use, communicated, published or admitted in evidence.

218. Paragraph 45(5) (a) provides that where protected information that has been disclosed in proceedings in open court, subsequent use, communication, publication or admission in evidence will not constitute an offence provided that the disclosure in court was lawful in the first place.

219. Paragraph 45(5) (b) provides that where protected information that has been used or communicated by a person who believes on reasonable grounds that the use or communication is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property, such use or communication will not constitute an offence. Such a person need not be a LEO.

220. Paragraph 45(5) (c) provides that communication to the Director-General (within the meaning of the *Australian Security Intelligence Organisation Act 1979* Cth) of protected information that relates or appears to relate to activities prejudicial to security (within the meaning of that Act) will not constitute an offence.

221. Paragraph 45(5)(d) provides that communication to an agency head of an agency (both terms are defined in the *Intelligence Services Act 2001*) of protected

information that relates or appears to relate to the functions of either organisation (within the meaning of that Act) will not constitute an offence.

222. Paragraph 45(5)(e) provides that the use, recording or communication of information referred to in paragraph (c) or (d) by an officer or employee of the Australian Security Intelligence Organisation (ASIO) or staff member of an agency (within the meaning of the *Intelligence Services Act 2001)* in the performance of his or her official functions will also not constitute an offence.

223. Paragraphs 45(5)(c), (d) and (e) provide for the communication of protected information to the Director-General of ASIO or the head of an agency within the meaning of the *Intelligence Services Act 2001* and its subsequent use by an officer, employee or staff member of ASIO or an agency for the purposes of protecting Australia's security interests.

224. Paragraphs 45(5)(f) provides for the communication of information to, and the use of information by, a foreign country in accordance with the *Mutual Assistance in Criminal Matters Act 1987* Cth (the MA Act), provided that such communication or use in respect of an offence against a law of that foreign country that is punishable by a maximum term of imprisonment of three years or more or for life or by death; this is because the threshold for communication of material to a foreign jurisdiction should be no lower than the threshold for communication to an Australian State.

225. Subclause 45(5) provides for a set of circumstances, related more closely to law enforcement, for which protected information may be lawfully used, recorded communicated, published or admitted in evidence.

226. Paragraph 45(5)(a) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of the investigation of a relevant offence, including a State or Territory relevant offence. A 'relevant offence' is defined in clause 6 of the Bill, a 'State or Territory relevant offence' is defined in subclause 45(9). It also allows for the making of a report with respect to such an investigation. This exception does not apply where paragraphs 45(5)(d) or 45(5)(h) would apply.

227. Paragraph 45(5)(b) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of making a decision whether or not to bring a prosecution of a relevant offence, including a State or Territory relevant offence. A 'relevant offence' is defined in clause 6 of the Bill, a 'State or Territory relevant offence' is defined in subclause 45(9). This exception does not apply where paragraphs 45(5)(d) or 45(5)(h) would apply.

228. Paragraph 45(5)(c) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of bringing a relevant proceeding, including a State or Territory relevant proceeding. A 'relevant proceeding' is defined in clause 6 of the Bill, a 'State or Territory relevant proceeding' is defined in subclause 45(9). This exception does not apply where paragraphs 45(5)(d) or 45(5)(h) would apply.

229. Paragraph 45(5)(d) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of an investigation of a complaint against, or into the conduct of, a public officer within the meaning of this Act. A 'public officer' is defined in clause 6. The paragraph also clarifies that the use, recording, communication, publication or admission in evidence of protected information is also permitted for the purpose of any subsequent investigation or prosecution of a relevant offence arising directly from the first-mentioned investigation, despite the fact such a use, recording, communication, publication or admission in evidence of protected information would otherwise not be permitted under this section.

230. Paragraph 45(5)(e) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of the making of a decision in relation to the appointment, re-appointment, term of appointment, termination or retirement of a person referred to in paragraph (d).

231. Paragraph 45(5)(f) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of the keeping of records and the making of reports by a LEA in accordance with the obligations imposed by Division 2 of Part 6 of this Bill.

232. Paragraph 45(5)(g) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of an inspection by the Commonwealth Ombudsman under clause 55 of the Bill.

233. Paragraph 45(5)(h) allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of allows for the use, recording, communication, publication or admission in evidence of protected information for the purposes of an investigation under the *Privacy Act 1988* (Cth) or any other law of the Commonwealth concerning the privacy of personal information. The paragraph also clarifies that the use, recording, communication, publication or admission in evidence of protected information is also permitted for the purpose of any subsequent investigation or prosecution of a relevant offence arising directly from the first-mentioned investigation, despite the fact such a use, recording, communication, publication or admission in evidence of protected information would otherwise not be permitted under this section.

234. Subclause 45(6) provides that the exceptions to be found in paragraphs 45(4)(f) and 45(5)(a),(b) and (c) do not apply to the use, recording, communication or publication of protection information that falls within paragraph 44(d) even if that information also falls within paragraphs 44(b) and 44(c). This is because protected information that falls within paragraph 44(d) has been improperly or illegally obtained and is therefore subject to a narrower set of exceptions than other types of protected information.

235. Protected information that falls within paragraph 44(d) may still be used, recorded, communicated or published under the exceptions contained in 45(4)(a),(b),(c),(d) and (e) because of the overriding public or national security interest in each case. Similarly, such information may also be communicated under the exceptions contained in 45(5)(d), (e), (f), (g) and (h) because these exceptions

allow for investigations into any improprieties which may attach to the surveillance itself or any subsequent use of protected information which have been gathered through that surveillance.

236. Paragraph 45(6)(b) provides that protected information which falls within paragraph 44(d) may not be given in evidence so as to maintain the public interest in evidence in a prosecution being free of any improprieties insofar as this is possible.

237. Subclause 45(7) provides that protected information obtained through the use of a SD by a LEO of a particular LEA and that is communicated to another LEA, or an agency that is not a LEA, may only be communicated within that second agency for the purpose for which it was communicated and it may not, except for the purpose of bringing a relevant proceeding, be communicated to any person who is not a member of that second agency. This is intended to protect the privacy of groups or individuals who may have recorded or monitored using a surveillance device..

238. Subclause 45(8) provides that a reference in 45(5) to a relevant offence is a reference to any relevant offence, whether or not the offence in respect of which the relevant warrant or emergency authorisation was issued or given. This means that if, for example, a SD warrant was issued with respect to a narcotics offence, any material gathered under that warrant may be communicated, subject to 45(5), with respect to any other relevant offence to which it relates, whether or not that offence is also a narcotics offence.

239. Subclause 45(9) defines various terms used in this clause.

240. ‘State or Territory relevant offence’ means an offence against the law of a State or of a self-governing Territory that is punishable by a maximum term of imprisonment of three years or more or for life. It is defined here because such an offence may serve as the basis for communication of protected material but not as the basis for a warrant or authorisation under this Bill.

241. ‘State or Territory relevant proceeding’ is similar to the definition of relevant proceeding in clause 6 but excludes those types of proceedings which are limited to the Commonwealth jurisdiction. It is defined here because such a proceeding may serve as the basis for communication of protected material.

Clause 46 Dealing with records obtained by use of surveillance devices

242. Paragraph 46(1)(a) imposes a duty upon the chief officer of a LEA to ensure that every record or report obtained by use of SD under a warrant, an emergency authorisation or a TD authorisation or that has been communicated to the agency by one of the exceptions in subclause 45(4) or 45(5), is kept in a secure place which is not accessible to those who are not entitled to deal with that record or report.

243. Paragraph 46(1)(b) further imposes an obligation upon the chief officer to destroy or cause to be destroyed any record or report obtained under paragraph 46(1)(a) if that person is satisfied that the record or report is not likely to be required in connection with a purpose referred to in subclause 45(3) or 45(5).

244. Subclause 46(2) imposes the same duties that the chief officer of a LEA has under subclause 46(1) on the officers in charge of an agency that is not a LEA. Such an agency might be, for example, the Commonwealth Director of Public Prosecutions or the Australian Taxation Office.

245. Subclause 46(3) clarifies subclauses 1 and 2 do not apply to records or reports that are received into evidence in legal or disciplinary proceedings.

Clause 47 Protection of Surveillance Device Methodologies

246. Clause 47 gives protection to sensitive information relating to surveillance device methodologies to prevent the release of such information to the public domain in a way that might harm future law enforcement operations.

247. Subclause 47(1) provides that a person may object during proceedings to the disclosure of information which, if disclosed could reasonably be expected to reveal details of surveillance device technology or methods of installation, use or retrieval of surveillance devices. In this clause, the reference to 'proceeding' is defined in subclause 47(7).

248. Subclause 47(2) allows for the person presiding over the proceedings, be he or she a Judge, Magistrate, Tribunal member or Royal Commissioner or any other type of presiding officer, may order that the person who has the information not be required to disclose it in the proceeding.

249. Subclause 47(3) provides the person presiding over the proceedings must consider whether the disclosure of information is necessary for the fair trial of the defendant or is otherwise in the public interest. The protection offered by this provision is therefore not absolute and the public interest in protecting sensitive law enforcement information must be weighed against other public interest concerns.

250. Subclause 47(4) is a saving provision which provides that this clause does not affect any other law under which a law enforcement officer cannot be compelled to disclose information or make statements in relation to the information.

251. Subclause 47(5) requires the person presiding over the proceeding to make any order they consider necessary to protect surveillance device methodologies that have been disclosed from being published.

252. Subclause 47(6) provides that the obligation imposed by subclause 47(5) is not absolute and does not apply if an order under subclause 47(5) would conflict with the interests of justice.
Subclause 47(8) defines 'proceeding' for the purposes of this clause to include any proceeding before a court, Tribunal or Royal Commission.

Clause 48 Protected information in the custody of a court, tribunal or Royal Commission

253. Clause 48 clarifies that a person is not entitled to search any protected information held in the custody of a court, tribunal or Royal Commission unless that

body orders otherwise in the interests of justice. Such information may be in the possession of a court, tribunal or Royal Commission because of an application for a warrant, for example. It is not appropriate, therefore, to allow such records to be searched unless the court, tribunal or Royal Commission is satisfied that such access is necessary in the interests of justice.

Division 2 – Reporting on each warrant or authorisation

Clause 49 Report on each warrant or authorisation

254. This clause sets out the reporting requirements incumbent upon the chief officer of each LEA to which an LEO belongs or is seconded to whom a warrant or an emergency or TD authorisation is issued. This ensures that LEAs are accountable for the use of SDs under warrants and authorisations.

255. Under subclauses 49(1)(d) and (e), the chief officer must, as soon as practicable after the warrant or authority ceases to be in force, make a report to the Minister setting out the requirements listed in subclauses 49(2) and (3) and give the Minister a copy of each warrant or authorisation, in addition to any instruments of revocation, extension or variation of each warrant or authorisation.

256. For SD warrants, emergency or TD authorisations, the report must state whether the warrant or authorisation was in fact executed and, if it was, the name of the person who was primarily responsible for its execution, the names of each person involved in the installation, maintenance or retrieval of the SD, amongst other things. The report must also detail persons who were surveilled and premises (including vehicles) or objects on which SDs were installed or used.

257. Importantly, for accountability purposes and in recognition of the balance that must be struck between law enforcement and the right to privacy, the report to the Minister must be provided so that it demonstrates the benefit to the investigation of the use of the SD and of the use made or to be made of any evidence or information stemming from the use of the SD. The report must also state the details of the communication of evidence or information obtained by the use of the SD to persons other than officers of the LEA.

258. Where a warrant or authorisation was extended or its terms varied, the nature of these must also be included in the report.

259. Clause 49(3) provides the details which the report must contain for retrieval warrants, which includes whether the SD was in fact retrieved and, if not, why it was not. The report must also specify details of any premises that were entered or anything that was opened or any object removed or replaced under the warrant. Compliance with the conditions that may have been imposed on the warrant must also be included.

Clause 50 Annual reports

260. Subclause 50(1) paragraphs (a) – (k) set out the reporting requirements that are to be provided for each financial year to the Minister by the chief officer of the LEA.
272. These include the number of warrants applied for and issued to LEOs of the LEA during the year, the number of emergency and TD authorisations applied for and issued in that year. This information must be specified in such a way as to enable the identification of the number of warrants issued, emergency authorisations and TD authorisations given in respect of each different kind of SD (subclause 50(2)).

261. The report must also specify the number of warrants and authorisations that were refused in the year and the reasons for their refusal.

262. As a measure of the usefulness of the SD regime and to gauge whether the right balance between law enforcement and intrusion into privacy has been struck, the number of arrests made by LEOs on the basis, either wholly or in part, of information obtained by the use of the SD under a warrant or authorisation must be included in the yearly report.

263. The compliance of LEOs with processes established by the SD Bill for obtaining and executing a SD warrant or authorisation can be measured, in part, by the number of prosecutions for relevant offences that were commenced and the number which resulted in a finding of guilt, which is also to be contained in the report.

264. The report is to be submitted to the Minister as soon as practicable, within a three month period, following the end of each financial year (subclause 50(3)).

265. Subclause 50(4) provides that the Minster is to table the report before both houses of Parliament within 15 sitting days of that House, after the Minister has received the report.

Clause 51 Keeping documents connected with warrants and emergency authorisations

266. This clause provides that the chief officer of a LEA must ensure that documents associated with SD warrants, emergency authorisations and TD authorisations are retained, including each warrant, emergency authorisation or TD authorisation issued and the applications upon which they were based. Applications made under clause 33 for the approval of the giving of an emergency authorisation must also be retained.

267. Instruments of revocation given to the chief officer under clauses 20 and 27 must also be retained, as well as a copy of each report submitted to the Minister under clause 49.

268. Documents relating to the extension, variation or revocation of a warrant and those concerned with court approval of emergency authorisation must also be retained.

Clause 52 Other records to be kept

269. This clause lists the documents that the chief officer of a LEA is required to ensure are kept. They pertain to the decision to grant, refuse or withdraw a SD warrant, an emergency or TD authorisation.

270. Records relating to the use and communication of information obtained under a SD are also to be documented and retained. This includes details of each communication by a LEO to another person who is not a LEO of their LEA, details of each occasion when information obtained under a SD by a LEO was given in a relevant proceeding or used for the location and safe recovery of a child under a recovery order.

271. Paragraph (j) states that the destruction of records or reports under clause 46(1)(b) must also be retained.

Clause 53 Register of warrants, emergency authorisations and tracking device authorisations

272. This clause requires the chief officer of a LEA to cause a register of warrants and emergency and TD authorisations sought by LEOs of their agency to be kept. This clause specifies the different requirements that the register must include for SD warrants, emergency authorisations and TD authorisations. The register is intended to provide an overview for the Ombudsman who is empowered to inspect such records under Division 3.

273. Subclause 53(2) states that the register must include details of each warrant issued, including the date the warrant was issued. It is also to include the name of the eligible Judge or nominated AAT member who issued or refused to issue the warrant, the name of the LEO named in the warrant as being primarily responsible for its execution, whether the warrant was issued for the investigation of a relevant offence or for the enforcement of a recovery order, the period it remained in fore and details of variations and extensions granted.

274. Subclause 53(3) provides that the register must specify, in relation to emergency authorisations, many of the details that are required to be kept for SD warrants. Whether the approval of powers exercised under the authorisation was granted or not and the date on which the application was approval must also be recorded.

275. Subclause 53(4) specifies what the register must contain for TDs. These include the date the TD authorisation was given or refused and the name of the appropriate authorising officer who issued or refused the authorisation. If a TD authorisation was issued, the register must include the name of the LEO to whom it was issued and whether the authorisation was issued for the purpose of an investigation of a relevant offence, or for the enforcement of a recovery order.

Division 3 – Inspections

Clause 54 Appointment of inspecting officers

276. This clause allows the Ombudsman to appoint members of the Ombudsman's staff to be inspecting officers for the purpose of this Division. The appointment must be evidenced in writing.

Clause 55 Inspection of records

277. This clause establishes an inspection regime by the Commonwealth Ombudsman who is empowered to inspect the records kept by LEAs. The role of the Ombudsman is to determine whether the records kept are accurate and whether the LEA is compliant with its reporting obligations.

278. Subclause 55(2) provides that the Ombudsman can enter premises occupied by the LEA at any reasonable time after notifying the chief officer of the agency. The Ombudsman is then entitled to full and free access at all reasonable times to all records of the LEA that are relevant to their inspection.

279. The Ombudsman has the power under subclause 55(2)(d) to require a member of staff of the LEA to provide any information relevant to the inspection that is in their possession or to which the member has access.

280. The chief officer is obligated to ensure that their staff provide the Ombudsman with any assistance that the Ombudsman reasonably requires enabling the Ombudsman to perform their functions.

281. Subclause 55(4) provides that the Ombudsman can choose to refrain from inspecting records of the LEA that concern obtaining or the execution of a warrant or authorisation while an operation is being presently being conducted under that warrant or authorisation. This is to avoid interfering in a current operation.

Clause 56 Power to obtain relevant information

282. This clause empowers the Ombudsman to require a LEO to provide information to the Ombudsman in writing, signed by the LEO, at a specified place and within a specified period of time where the Ombudsman has reason to believe that the LEO is able to give the information required. Under subclause 56(2), the Ombudsman must write to the LEO to do so.

283. Under subclause 56(3) the Ombudsman may also require (by writing) an officer to answer questions before a specified inspecting officer at a specified place and within a specified period, or at a particular time on a particular day.

284. Subclause 56(4) also authorises the Ombudsman to write to the chief officer of a LEA to require them, or a person nominated by the chief officer, to answer

questions relevant to the inspection before a specified inspecting officer, at a specified place and within a specified period, or at a particular time on a particular day, which is reasonable having regard to the circumstances in which the requirement is made as required by subclause 56(5). The Ombudsman can only do this where they have reason to believe that a LEO, whose identity in unknown to the Ombudsman, is able to give information relevant to an inspection under Division 3.

285. Subclause 56(6) establishes an offence where a person refuses to attend before a person, refuses to give information or answer questions when required to do so under clause 56. The penalty for the offence is imprisonment for six months.

Clause 57 Ombudsman to be given information and access notwithstanding other laws

286. Subclause 57 (1) states that a person is not excused from providing information, answering questions or giving access to a document either when required or under Division 3, on the grounds that doing so would contravene a law, would be contrary to the public interest or might tend to incriminate the person or make them liable to a penalty. However, the information provided, the answer given or the fact that the person has given access to a document, and any information or thing that is obtained as a direct or indirect consequence, is not admissible in evidence against the person except in a proceeding against clause 45 of the Bill (which relate to offences regarding the use, recording, communication or publication of protected information) or against Part 7.4 or 7.7 of the Criminal Code, which relate to hindering, obstructing, intimidating or resisting a public official in the performance of their functions.

287. Subclause 57(2) provides that nothing in clause 45, which relates to the prohibition on use, communication or publication of protected information or its admission in evidence, or any other law prevents a LEO from providing information to an inspecting officer in any form or from providing access to records of the LEA for the purposes of inspection under Division 3.

288. Subclause 57(2) adds to this by providing that nothing in clause 45, or any other law, prevents an officer of a LEA from making a record of information, or causing such a record to be made for the purposes of giving the information to a person as permitted by subclause (2).

Clause 58 Exchange of information between Ombudsman and State inspecting authorities

289. This clause and clause 59 allow the Commonwealth to develop more effective and consistent inspection arrangements with other inspecting bodies, particularly State Ombudsmen.

290. Subclause 58(1) provides definitions for ‘State or Territory agency’ and ‘State or Territory inspecting authority’ for the purposes of clause 58.

291. Subclause 58(2) authorises the Ombudsman to give information that relates to a State or Territory agency which was obtained by the Ombudsman under this Act to the inspecting authority in relation to the agency in the relevant State or Territory.

Under subclause 58(3), the information can only be passed where the Ombudsman believes the information is necessary for the inspecting authority to perform its functions in relation to the State or Territory agency.

292. Conversely, under subclause 58(4), the Ombudsman can receive from a State or Territory inspecting authority information relevant to the performance of the Ombudsman's functions under this Act.

Clause 59 Delegation by Ombudsman

293. This clause and clause 58 allow the Commonwealth to develop more effective and consistent inspection arrangements with other inspecting bodies, particularly State Ombudsmen.

294. Subclause 59 (1) authorises the Ombudsman to delegate some or all of their powers under Division 3, except the power to report to the Minister and the power of delegation under this clause. The delegation can be to an APS employee who is responsible to the Ombudsman or to a person holding an equivalent office to the Ombudsman under a State or Territory law or to an employee who is responsible to that person. The delegation can be of a general nature or be exercised within terms provided by an instrument of delegation.

295. Subclause (2) states that a delegate under Division 3 is to provide a copy of the delegation instrument for inspection by a person who is affected by the exercise of any power so delegated if a request to see it is made.

Clause 60 Ombudsman not to be sued

296. This clause gives immunity from action, suit or proceeding to the Ombudsman, an inspecting officer or a person acting under an inspecting officer's direction or authority for an act or omission that was done, or not done, in good faith in the performance or exercise, purported or otherwise, of a function, power or authority conferred under Division 3.

Clause 61 Report on inspection

297. Under this clause, the Ombudsman is required to produce a written report to the Minister every six months containing the results of each inspection undertaken under clause 54. Therefore an inspection by the Ombudsman required by clause 55 must be at least six-monthly.

298. Subclause 61(2) provides that a copy of the Ombudsman's report is to be tabled by the Minister before each House of Parliament within 15 sitting days of that House after the Minister has received the report.

Division 4 – General

Clause 62 Evidentiary certificates

299. Subclause 62(1) allows an appropriate authorising officer, or a person assisting them, to issue an evidentiary certificate. Such a certificate is intended to streamline the court process because it will reduce the need to call numerous LEOs and expert technical witness to give evidence about routine matters concerning the execution of warrants and the use of information obtained from the SDs.

300. The certificate may contain any facts that the issuer considers relevant, including anything done by a LEO or by a person providing technical assistance in connection with a warrant's execution or anything done in accordance with an emergency or TD authorisation (subclause 62(1)(a)).

301. The certificate may also set out relevant facts with respect to anything done by a LEO relating to the communication of SD product obtained under a warrant or emergency or TD authorisation by a person to another person. A certificate can also set out anything done by a LEO concerning the making of a record or the custody of a record of SD product obtained under a warrant or authorisation.

302. Under subclause 63(2), a certificate purporting to be a certificate issued under subclause 62(1) is admissible in evidence in any proceeding as prima facie evidence of the matters stated in the certificate.

303. Subclause 62(3) provides that a certificate which sets out facts in connection with anything done under an emergency authorisation is only to be a certificate which will be admissible in evidence in any proceedings if the emergency authorisation has been approved under clause 35.

304. Subclause 62(4) provides that a certificate issued under subclause (1) is to be taken as an evidentiary certificate and to have been duly given, unless the contrary intention is established.

305. Under subclause 62(5), an evidentiary certificate is not to be admitted in evidence under subsection (2) in prosecution proceedings unless the person charged with the offence, or a solicitor who has appeared for the person in those proceedings, has, at least 14 days before the certificate is sought to be admitted, been given a copy of it together with reasonable evidence of the intention to produce the certificate as evidence in the proceedings.

306. Subclause 62(6) provides that, subject to subclause 62(7), if a certificate is admitted in prosecution proceedings as prima facie evidence of the matters sated in it, the person charged with the offence may require the person giving the certificate to be called as a witness for the prosecution and cross-examined as if he or she had given evidence of the matters stated in the certificate.

307. Subclause 62(7) states that subclause 62(6) does not entitle the person charged to require the person who gave an evidentiary certificate to be called as a witness for the prosecution unless the court orders that the person charged be allowed to require the person giving the certificate to be called.

308. Subclause 62(8) states that any evidence in support or otherwise of a matter stated in a certificate must be considered on its merits and the credibility and

probative value of such evidence must be neither increased or diminished by reason of this section.

PART 7 - MISCELLANEOUS

Clause 63 Delegation by chief officer of law enforcement agency

309. This clause provides that a chief officer of a LEA can delegate to a member of staff who is an SES employee or a person of equivalent rank within the agency, all or any of their powers and functions under the SD Bill.

Clause 64 Regulations

310. Subclause 64(1) provides that the Governor-General may make regulations prescribing matters that are either required or permitted by the SD Bill to be so prescribed. The Governor-General can further prescribe matters necessary or convenient for carrying out or giving effect to the Bill.

311. Such regulations may impose a penalty, not exceeding 50 penalty units, for a contravention of the regulations.

Schedule 1 Amendment of other legislation and transitional provisions

Australian Federal Police Act 1979

1. Division 2 of Part II

This item repeals part II of Division 2 of the AFP Act.

2. Transitional and saving provision

This provision establishes the relationship between the SD Bill and the old law under the AFP Act. It sets out the application of the SD Bill to matters that arose before the alteration to the AFP Act. For example, paragraph (a) provides deals with the validity of warrants issued under Division 2 of the AFP Act that are in force before the repeal. Following the repeal, such warrants are to remain in force according to their terms as if the Division had not been repealed.

Paragraphs (b), (c) and (d) set out to what extent nominations and consents under Division 2 of the AFP Act are to have effect under the Bill. Specifically, paragraph (b) provides that any consent given by a Judge of a court created by the Parliament to be nominated under subsection 12D(2) of the AFP Act which is in force prior to the repeal of Division 2, is to be treated from the day of repeal as if it was a consent under subclause 12(3) of the SD Bill.

Similarly, paragraph (c) provides that any nomination by the Minister of a Judge of a court created by the Parliament under section 12G of the AFP Act which is in force prior to the repeal of Division 2, is to be treated from the day of repeal as if it was a nomination under clause 12 of the SD Bill.

Paragraph (d) provides that any nomination by the Minister of a person holding an appointment referred to in subsection 12DA(1) of the AFP Act which is in force prior to the day of repeal, is to be taken as if it were a nomination of that person for the purposes of clause 13 of the SD Bill.

3. Operation of Division 2 of Part II of the Australian Federal Police act 1979 preserved or limited purposes

This item provides that, despite the repeal of Division 2, that Division is to be treated as continuing in its application to the use of LDs for offences against the law of the ACT. Paragraph (b) provides that, despite the repeal, definitions of various terms in Division 2 are to be taken as if they were limited to offences against the law of the ACT.

Paragraph (c) provides that, despite the repeal and for the purposes of the continued operation of section 12L of the AFP Act, sections 219F to 219K of the Customs Act are to be treated as having not been repealed. In addition, reference to section 12L of the AFP Act to general, class 1 general or class 2 general offences are to be construed as if they were limited to offences against ACT law.

Criminal Code Act 1995

4. Paragraph 476.2(4)(b) of the Schedule

This item provides that paragraph 476.2(4)(b) in the Schedule to the Criminal Code Act is to be repealed and replaced with the paragraph appearing in the Schedule of the SD Bill. This paragraph has the effect of including in the Code, reference to emergency and TD authorisations that had not previously been dealt with by the Code. In this way, access to data held in a computer, the modification of such data, the impairment of electronic communication to or from a computer, or the impairment of the reliability, security or operation of any data held on a computer disk, credit card or other device used to store data by electronic can be authorised by a warrant, emergency or TD authorisation.

This provision provides an immunity from the Computer Offences in Part 10.7 of the Code for Commonwealth or State law enforcement officers acting under a Commonwealth warrant, emergency authorisation (or State equivalent thereof) or a tracking device authorisation.

Customs Act 1901

5. Division 1A of Part XII

This Item repeals this Division.

6. Transitional and saving provision

In the same way as Item 2 does for the AFP Act, item 6 establishes the relationship between the new provisions relating to warrants, consent by Judges and nominations by the Minister under the SD Bill to the provisions which dealt with these matters under Division 1A of Part XII of the Customs Act.

Warrants issued under the Division are to remain in force according to their terms after the repeal as if the Division had not been repealed.

Consents by Judges and nominations by the Minister under the Customs Act are to be treated as if they were consents and nominations under the SD Bill in relation to eligible Judges or nominated AAT members.

Mutual Assistance in Criminal Matters Act 1987

7. 13A Requests by foreign countries for provision of material lawfully obtained

Foreign countries often request material that is in the lawful possession of law enforcement agencies, such as material obtained by consent or search warrant. Such material also includes protected information under clause 34 of the SD Bill. Clause 13A of the *Mutual Assistance in Criminal Matters Act 1987* (MA Act) streamlines the process for providing material in the lawful possession of law enforcement agencies to foreign countries without limiting alternative processes that may be available under the MA Act or otherwise.

Clause 13A provides an additional means of providing material to foreign countries under the MA Act. Clause 13A allows the Attorney-General to authorise material that is in the lawful possession of law enforcement agencies, other than telephone intercept material, being provided to foreign countries for foreign investigations and prosecutions. This avoids the need to apply to a court to provide to foreign countries material that has already lawfully been obtained by law enforcement agencies. The Attorney-General's authorisation under clause 13A may include a direction by the Attorney-General about how the material is to be dealt with by the law enforcement agency when providing it to a foreign country.

Material gathered under a telecommunications interception warrant is not included in this provision.

Australian law enforcement agencies can provide material to foreign countries on a police-to-police basis in certain circumstances. Clause 13A is not intended to limit the ability of law enforcement agencies to provide material on the basis of police-to-police assistance.