Serial 100
Surveillance Devices Bill 2007
Mr Stirling

A BILL
for
AN ACT

about the use of surveillance devices

NORTHERN TERRITORY OF AUSTRALIA

SURVEILLANCE DEVICES ACT 2007

Act No. [ ] of 2007

TABLE OF PROVISIONS

Section

NORTHERN TERRITORY OF AUSTRALIA

Act No. [ ] of 2007

AN ACT

about the use of surveillance devices

[*Assented to [ ] 2007*]
[*Second reading [ ] 2007*]

The Legislative Assembly of the Northern Territory enacts as follows:

PART 1 – INTRODUCTION

Division 1 – Preliminary matters

1. Short title

This Act may be cited as the *Surveillance Devices Act 2007*.

2. Commencement

This Act commences on the date fixed by the Administrator by *Gazette* notice.

3. Purpose

The purposes of this Act are:

(a) to regulate the installation, use, maintenance and retrieval of surveillance devices; and

(b) to restrict the use, communication and publication of information obtained through the use of surveillance devices or otherwise connected with surveillance device operations; and

(c) to establish procedures for law enforcement officers to obtain warrants or emergency authorisations for the installation, use, maintenance and retrieval of surveillance devices in criminal investigations extending beyond this jurisdiction; and

(d) to recognise warrants and emergency authorisations issued in other jurisdictions; and

(e) to impose requirements for the secure storage and destruction of records, and the making of reports to Judges, magistrates and Parliament, in relation to surveillance device operations.

Division 2 – Interpretation

4. Definitions

In this Act:

"applicant", for a warrant, means the law enforcement officer who applies, or on whose behalf an application is made, for the warrant;

"Australian Crime Commission" means the Australian Crime Commission established by the *Australian Crime Commission Act 2002* (Cth);

"authorised person" means a person holding an appointment under section 74;

"business day" means a day other than a Saturday, Sunday or public holiday;

"chief officer" means:

(a) for the Territory Police Force – the Commissioner of Police; or

(b) for the Australian Crime Commission – the Chief Executive Officer of the Australian Crime Commission;

"Commonwealth Ombudsman" means the person occupying or holding office as the Commonwealth Ombudsman under the *Ombudsman Act 1976* (Cth);

"computer" means any electronic device for storing or processing information;

"connection device" means a device that is not a surveillance device or part of a surveillance device but is ancillary to the installation, use, maintenance or retrieval of a surveillance device;

"corresponding emergency authorisation" means an authorisation in the nature of an emergency authorisation given under a corresponding law for a relevant offence under the law;

"corresponding law" means a law of another jurisdiction that:

(a) provides for the authorisation of the use of surveillance devices; and

(b) is declared by regulation to be a corresponding law;

"corresponding protected information", see section 51(3);

"corresponding warrant" means a warrant in the nature of a surveillance device warrant or retrieval warrant issued under a corresponding law for a relevant offence under the law;

"data surveillance device" means a device capable of being used to monitor or record the information being put on to or retrieved from a computer, but does not include an optical surveillance device;

"device" includes apparatus, equipment, instrument and machine;

"emergency authorisation" means an emergency authorisation given under section 35;

"emergency authorisation (serious drugs offence)" means an emergency authorisation given on an application made under section 33(2);

"emergency authorisation (serious violence)" means an emergency authorisation given on an application made under section 33(1);

"enhancement equipment", in relation to a surveillance device, means equipment capable of enhancing a signal, image or other information obtained by the use of the device;

"install" includes attach;

"jurisdiction" means a State or another Territory of the Commonwealth;

"law enforcement agency" means the following agencies:

(a) the Territory Police Force;

(b) the Australian Crime Commission;

"law enforcement officer" means:

(a) for the Territory Police Force:

(i) a police officer; or

(ii) a person who is seconded to the Police Force, including, for example, a member of the police force or police service or a police officer (however described) of another jurisdiction; or

(b) for the Australian Crime Commission:

(i) a member of staff of the Australian Crime Commission; or

(ii) a person who is seconded to the Commission, including, for example, a member of the police force or police service or a police officer (however described) of another jurisdiction;

"listening device" means a device capable of being used to listen to, monitor or record a conversation or words spoken to or by a person in a conversation, but does not include a hearing aid or similar device used by a person with impaired hearing to overcome the impairment and permit the person to hear only sounds ordinarily audible to the human ear;

"listen to" includes hear;

"local protected information", see section 51(2);

"maintain", in relation to a surveillance device, includes:

(a) adjust, relocate, repair or service the device; and

(b) if the device is faulty, replace it;

"offence" means an offence against the law of the Territory, the Commonwealth or another jurisdiction;

"on", a place or thing, includes at and in the place or thing;

"optical surveillance device" means a device capable of being used to monitor, record visually or observe an activity, but does not include spectacles, contact lenses or a similar device used by a person with impaired sight to overcome the impairment and permit the person to see only sights ordinarily visible to the human eye;

"participating jurisdiction" means a jurisdiction in which a corresponding law is in force;

"party" means:

(a) for a private conversation – a person by or to whom words are spoken in the course of the conversation; or

(b) for a private activity – a person who takes part in the activity;

"place" includes vacant land, premises and a vehicle;

"possess", for a surveillance device, includes having the source under control in any place, whether or not another person has the custody of the device.

"premises" includes the following, regardless of whether in or outside this jurisdiction:

(a) a building or structure;

(b) a part of a building or structure;

(c) land on which a building or structure is situated;

"private activity" means an activity carried on in circumstances that may reasonably be taken to indicate the parties to the activity desire it to be observed only by themselves, but does not include an activity carried on in circumstances in which the parties to the activity ought reasonably to expect the activity may be observed by someone else;

"private conversation" means a conversation carried on in circumstances that may reasonably be taken to indicate the parties to the conversation desire it to be listened to only by themselves, but does not include a conversation carried on in circumstances in which the parties to the conversation ought reasonably to expect the conversation may be overheard by someone else;

"protected information", see section 51(1);

"public officer" means a person employed by, or holding an office established by or under a law of, this jurisdiction or a person employed by a public authority of this jurisdiction, and includes a law enforcement officer;

"reasonably believes" means believes on grounds that are reasonable in the circumstances;

"record" includes:

(a) an audio, visual or audio visual record; and

(b) a record in digital form; and

(c) a documentary record prepared from a record mentioned in paragraph (a) or (b);

"relevant offence" means:

(a) an offence against a law of this jurisdiction punishable by imprisonment for a term of 3 years or more or for life; or

(b) an offence against a law of this jurisdiction prescribed by regulation;

"relevant proceeding" means:

(a) the prosecution of an offence; or

(b) a bail application or review of a decision to grant or refuse a bail application; or

(c) a proceeding for the committal of a person to stand trial for an offence; or

(d) a proceeding for the confiscation, forfeiture or restraint of property or for the imposition of a pecuniary penalty in relation to an offence, or a proceeding related or ancillary to such a proceeding; or

(e) a proceeding for the protection of a child or intellectually impaired person; or

(f) a proceeding concerning the validity of a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or

(g) a disciplinary proceeding against a public officer; or

(h) a coronial inquest or inquiry if, in the opinion of the coroner, the event the subject of the inquest or inquiry may have resulted from the commission of an offence; or

(i) a proceeding under section 13 of the *Mutual Assistance in Criminal Matters Act 1987* (Cth) in relation to a criminal matter concerning an offence against the laws of the foreign country making the request resulting in the proceeding; or

(j) a proceeding for the taking of evidence under section 43 of the *Extradition Act 1988* (Cth); or

(k) a proceeding for the extradition of a person from another jurisdiction to this jurisdiction; or

(l) a proceeding under Part 4, Division 1, of the *International War Crimes Tribunals Act 1995* (Cth);

(m) a proceeding of the International Criminal Court;

"remote application" for a warrant, means an application mentioned in section 20 or 28;

"report", of a conversation or activity, includes a report of the substance, meaning or purport of the conversation or activity;

"retrieval warrant" means a warrant issued under Part 4, Division 3;

"senior officer" means:

(a) for the Territory Police Force:

(i) the Commissioner of Police; or

(ii) a Deputy Commissioner of Police; or

(iii) an Assistant Commissioner of Police; or

(b) for the Australian Crime Commission – the Chief Executive Officer or an examiner as defined in the *Australian Crime Commission Act 2002* (Cth);

"serious drug offence" means an offence involving the possession, use, manufacture, production or supply of a dangerous drug as defined in the *Misuse of Drugs Act*;

"surveillance device" means:

(a) a data surveillance device, listening device, optical surveillance device or tracking device; or

(b) a device that is a combination of any 2 or more of the devices mentioned in paragraph (a); or

(c) a device of a kind prescribed by regulation;

"surveillance device warrant" means a warrant issued under Part 4, Division 2;

"this jurisdiction" means the Territory;

"tracking device" means an electronic device that may be used to determine the geographical location of a person or thing;

"unsworn application" for a warrant, means an application mentioned in section 19(4) or 27(4);

"use", of a surveillance device, includes use of the device to record a conversation or other activity;

"vehicle" means anything used for carrying any person or anything by land, water or air;

"warrant" means surveillance device warrant or retrieval warrant.

5. Law enforcement officer primarily responsible for warrant

In this Act, a reference to the law enforcement officer primarily responsible for executing a warrant is a reference to the officer named in the warrant as such, whether or not the officer is physically present for any step in the execution of the warrant.

6. Cross-border investigations taken to be carried out in this jurisdiction

For this Act, an investigation into an offence is taken to be conducted in this jurisdiction (whether or not it is also conducted in another jurisdiction) if a law enforcement officer participates in the investigation.

7. Declared offences for Criminal Code

An offence against this Act is an offence to which Part IIAA of the Criminal Code applies.

Note

Part IIAA of the Criminal Code states the general principles of criminal responsibility (including burdens of proof and general defences) and defines terms used for offences.

Division 3 – Application of Act

8. Act binds Crown

This Act binds the Crown in right of the Territory and, to the extent the legislative power of the Legislative Assembly permits, the Crown in all its other capacities.

9. Act does not apply to certain Commonwealth agents

This Act does not apply to anything done in the course of duty by:

(a) a member or member of staff of the Australian Competition and Consumer Commission; or

(b) the Director General or an officer or employee of the Australian Security Intelligence Organisation; or

(c) a member of the Australian Federal Police, other than in the member's capacity as a member of staff of the Australian Crime Commission; or

(d) an officer of customs as defined in the *Customs Act 1901* (Cth); or

(e) the Minister administering the *Migration Act 1958* (Cth) or the Secretary or an officer or employee of the Department as defined in that Act.

10. Act does not limit court discretion

(1) This Act is not intended to limit a discretion that a court has:

(a) to admit or exclude evidence in any proceeding; or

(b) to stay a criminal proceeding in the interests of justice.

(2) To avoid doubt, it is intended that a warrant may be issued, or an emergency authorisation given, in this jurisdiction under this Act for the installation, use, maintenance or retrieval of a surveillance device in this jurisdiction or a participating jurisdiction or both.

(3) Subsection (2) is subject to sections 23(8) and 36(2).

PART 2 – REGULATION OF INSTALLATION, USE AND MAINTENANCE OF SURVEILLANCE DEVICES

11. Installation, use and maintenance of listening devices

(1) A person is guilty of an offence if the person:

(a) installs, uses or maintains a listening device to listen to, monitor or record a private conversation to which the person is not a party; and

(b) knows the device is installed, used or maintained without the express or implied consent of each party to the conversation.

Maximum penalty: 250 penalty units or imprisonment for 2 years.

(2) Subsection (1) does not apply to:

(a) the installation, use or maintenance of a listening device under:

(i) a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or

(ii) under a law of the Commonwealth; or

(b) the use of a listening device by a law enforcement officer to monitor or record a private conversation to which the officer is not a party if:

(i) at least 1 party to the conversation expressly or impliedly consents to the monitoring or recording; and

(ii) the officer is acting in the performance of the officer's duty; and

(iii) the officer reasonably believes it is necessary to monitor or record the conversation for the protection of someone's safety; or

(c) the use of a listening device under section 43.

12. Installation, use and maintenance of optical surveillance devices

(1) A person is guilty of an offence if the person:

(a) installs, uses or maintains an optical surveillance device to monitor, record visually or observe a private activity to which the person is not a party; and

(b) knows the device is installed, used or maintained without the express or implied consent of each party to the activity.

Maximum penalty: 250 penalty units or imprisonment for 2 years.

(2) Subsection (1) does not apply to the installation, use or maintenance of an optical surveillance device:

(a) under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or

(b) under a law of the Commonwealth; or

(c) by a law enforcement officer in the performance of the officer's duty on a place if:

(i) an occupier of the place authorises the installation, use or maintenance; and

(ii) the installation, use or maintenance is reasonably necessary for the protection of someone's lawful interests; or

(d) the use of an optical surveillance device by a law enforcement officer in the performance of the officer's duty if it does not involve the following without permission:

(i) entry on a place;

(ii) interference with a vehicle or other thing; or

(e) the use of an optical surveillance device under section 44.

13. Installation, use and maintenance of tracking devices

(1) A person is guilty of an offence if the person:

(a) installs, uses or maintains a tracking device to determine the geographical location of a person or thing; and

(b) knows the device is installed, used or maintained without the express or implied consent of:

(i) for a device to determine the location of a person – the person; or

(ii) for a device to determine the location of a thing – a person in lawful possession or having lawful control of the thing.

Maximum penalty: 250 penalty units or imprisonment for 2 years.

(2) Subsection (1) does not apply to the installation, use or maintenance of a tracking device:

(a) under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or

(b) under a law of the Commonwealth; or

(c) if the device is installed by a law enforcement officer in the performance of the officer's duty on a thing when the thing is in a public place; or

(d) if the device is installed, used or maintained in prescribed circumstances.

14. Installation, use and maintenance of data surveillance devices by law enforcement officers

(1) A law enforcement officer is guilty of an offence if the officer:

(a) installs, uses or maintains a data surveillance device to monitor or record the input of information into, or the output of information from, a computer; and

(b) knows the device is installed, used or maintained without the express or implied consent of the person on whose behalf the information is being input or output.

Maximum penalty: 250 penalty units or imprisonment for 2 years.

(2) Subsection (1) does not apply to the installation, use or maintenance of a data surveillance device:

(a) under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation; or

(b) under a law of the Commonwealth.

PART 3 – RESTRICTION ON COMMUNICATION AND PUBLICATION OF PRIVATE CONVERSATIONS AND ACTIVITIES

15. Communication and publication of private conversations and activities

(1) A person is guilty of an offence if the person:

(a) communicates or publishes a record or report of a private conversation or private activity; and

(b) knows the record or report has been made as a direct or indirect result of the use of a listening device, optical surveillance device or tracking device.

Maximum penalty: 250 penalty units or imprisonment for 2 years.

(2) Subsection (1) does not apply:

(a) to a communication or publication made with the express or implied consent of each party to the private conversation or private activity; or

(b) to a communication or publication that is reasonably necessary:

(i) in the public interest; or

(ii) for protecting the lawful interests of the person making it; or

(c) to a communication or publication in the course of a legal or disciplinary proceeding; or

(d) to a communication or publication of protected information; or

(e) to a communication or publication made by a law enforcement officer:

(i) to a person authorised by the chief officer of the law enforcement agency for investigating or prosecuting an offence; or

(ii) to the occupier of a place of a record or report of a private activity made as a direct or indirect result of the use on the place of an optical surveillance device in the circumstances mentioned in section 12(2)(c); or

(iii) otherwise in the performance of the officer's duty; or

(f) to a communication or publication authorised by a law of the Commonwealth relating to the security of the Commonwealth.

16. Communication and publication of information from use of data surveillance device

(1) A law enforcement officer is guilty of an offence if:

(a) the officer communicates or publishes any information (the "relevant information") about the input of information into, or the output of information from, a computer; and

(b) the relevant information has been obtained as a direct or indirect result of the use of a data surveillance device.

Maximum penalty: 100 penalty units or imprisonment for 1 year.

(2) Subsection (1) does not apply:

(a) to a communication or publication made with the express or implied consent of the person for whom the information is input into or output from the computer; or

(b) to a communication or publication made in the course of a legal or disciplinary proceeding; or

(c) to a communication or publication of protected information; or

(d) to a communication or publication made by a law enforcement officer:

(i) to a person authorised by the chief officer of the law enforcement agency for investigating or prosecuting an offence; or

(ii) otherwise in the performance of the officer's duty; or

(e) to a communication or publication authorised by a law of the Commonwealth relating to the security of the Commonwealth.

PART 4 – WARRANTS FOR USE OF SURVEILLANCE DEVICES

Division 1 – Introduction

17. Types of warrant

(1) The following types of warrant may be issued under this Part:

(a) a surveillance device warrant;

(b) a retrieval warrant.

(2) A warrant may be issued for more than 1 surveillance device of the same or different kinds.

18. Who may issue warrant

(1) A Judge may issue any warrant under this Part.

(2) A magistrate may issue:

(a) a surveillance device warrant that authorises the use of a tracking device only; or

(b) a retrieval warrant for a tracking device authorised under a warrant mentioned in paragraph (a) if a magistrate issued the original warrant.

Division 2 – Surveillance device warrants

19. Application for surveillance device warrant

(1) A law enforcement officer (or another person on the officer's behalf) may apply for the issue of a surveillance device warrant if the law enforcement officer reasonably believes:

(a) an offence has been, is being, is about to be or is likely to be committed; and

(b) the use of a surveillance device is or will be necessary for the purpose of an investigation into the offence or of enabling evidence or information to be obtained of the commission of the offence or the identity or location of the offender.

(2) The application may be made to:

(a) a Judge in any case; or

(b) a magistrate in the case of an application for a warrant authorising the use of a tracking device only.

(3) The application must:

(a) state the name of the applicant; and

(b) state the nature and duration of the warrant sought, including the kind of surveillance device sought to be authorised; and

(c) be supported by an affidavit stating the grounds on which the warrant is sought.

(4) However, the application may be made before an affidavit is prepared or sworn if the applicant reasonably believes:

(a) the immediate use of a surveillance device is necessary for a purpose mentioned in subsection (1)(b); and

(b) it is impracticable for an affidavit to be prepared or sworn before an application is made.

(5) If subsection (4) applies, the applicant must:

(a) give as much information as the Judge or magistrate considers is reasonably practicable in the circumstances; and

(b) not later than the day following the making of the application, send a duly sworn affidavit to the Judge or magistrate, regardless of whether a warrant is issued.

(6) The Judge or magistrate may require the applicant or another person to give, either orally or by affidavit, further information in support of the application.

(7) An application for a warrant must not be heard in open court.

20. Remote application

(1) If a law enforcement officer reasonably believes it is impracticable for an application for a surveillance device warrant to be made in person, the application may be made under section 19 by phone, fax, email or another form of communication.

(2) Subsection (3) applies if:

(a) an affidavit has been prepared (whether sworn or unsworn); and

(b) when making the application, the applicant has access to a fax or email facility.

(3) The applicant must fax or email a copy of the affidavit with the application to the Judge or magistrate who is to decide the application.

21. Deciding application

(1) A Judge or magistrate may issue a surveillance device warrant if satisfied:

(a) there are reasonable grounds for the belief founding the application for the warrant; and

(b) in the case of an unsworn application – it would have been impracticable for an affidavit to have been prepared or sworn before it was made; and

(c) in the case of a remote application – it would have been impracticable for the application to have been made in person.

(2) In deciding whether a surveillance device warrant should be issued, the Judge or magistrate must have regard to:

(a) the nature and gravity of the alleged offence for which the warrant is sought; and

(b) the extent to which anyone's privacy is likely to be affected; and

(c) the existence of any alternative way of obtaining the evidence or information sought to be obtained and the extent to which that way may assist or prejudice the investigation; and

(d) the evidentiary or intelligence value of any information sought to be obtained; and

(e) any previous warrant sought or issued under this Division or a corresponding law (if known) in relation to the same offence.

22. What surveillance device warrant must contain

(1) A surveillance device warrant must:

(a) state that the issuing Judge or magistrate is satisfied of the matters mentioned in section 21(1) and has had regard to the matters mentioned in section 21(2); and

(b) state:

(i) the name of the applicant; and

(ii) the alleged offence for which the warrant is issued; and

(iii) the date the warrant is issued; and

(iv) the kind of surveillance device authorised to be used; and

(v) if the warrant authorises the use of a surveillance device on a place – the place; and

(vi) if the warrant authorises the use of a surveillance device on a thing or class of thing – the thing or class of thing; and

(vii) if the warrant authorises the use of a surveillance device for the activities, conversations or geographical location of a person – the name of the person or, if the identity of the person is unknown, the fact that the person's identity is unknown; and

(viii) the period (not exceeding 90 days) during which the warrant is in force; and

(ix) the name of the law enforcement officer primarily responsible for executing the warrant; and

(x) any conditions subject to which a place may be entered, or a surveillance device may be used, under the warrant; and

(xi) the time within which a report in relation to the warrant must be made to the Judge or magistrate under section 58.

(2) A warrant must be signed by the issuing Judge or magistrate and include the name of the Judge or magistrate.

(3) If the Judge or magistrate issues the warrant on a remote application, the Judge or magistrate must:

(a) tell the applicant of:

(i) the terms of the warrant; and

(ii) the date and time of its issue; and

(b) enter the details mentioned in paragraph (a) in a register kept by the Judge or magistrate for the purpose; and

(c) give the applicant a copy of the warrant as soon as practicable.

23. What surveillance device warrant authorises

(1) A surveillance device warrant may authorise, as stated in it, any 1 or more of the following:

(a) the use of a surveillance device on a stated place;

(b) the use of a surveillance device on a stated thing or class of thing;

(c) the use of a surveillance device for the activities, conversations or geographical location of a stated person or a person whose identity is unknown.

(2) A surveillance device warrant authorises:

(a) for a warrant of a kind mentioned in subsection (1)(a):

(i) the installation, use and maintenance of a surveillance device of the kind stated in the warrant on the stated place; and

(ii) the entry, by force if necessary, onto the place, or other stated place adjoining or providing access to the place, for any of the purposes mentioned in subparagraph (i) or subsection (3); or

(b) for a warrant of a kind mentioned in subsection (1)(b):

(i) the installation, use and maintenance of a surveillance device of the kind stated in the warrant on the stated thing or a thing of the stated class; and

(ii) the entry, by force if necessary, onto any place where the thing, or a thing of the class, is reasonably believed to be or is likely to be, or other place adjoining or providing access

to that place, for any of the purposes mentioned in subparagraph (i) or subsection (3); or

(c) for a warrant of a kind mentioned in subsection (1)(c):

(i) the installation, use and maintenance of a surveillance device of the kind stated in the warrant on a place where the person is reasonably believed to be or likely to be; and

(ii) the entry, by force if necessary, onto the place, or other place adjoining or providing access to that place, for any of the purposes mentioned in subparagraph (i) or subsection (3).

(3) A surveillance device warrant also authorises:

(a) the retrieval of the surveillance device; and

(b) the installation, use, maintenance and retrieval of any enhancement equipment in relation to the device; and

(c) the temporary removal of a thing from a place for the purpose of the installation, maintenance or retrieval of the device or equipment and the return of the thing to the place; and

(d) the breaking open of anything for the installation, maintenance or retrieval of the device or equipment; and

(e) the connection of the device or equipment to an electricity supply system and the use of electricity from that system to operate the device or equipment; and

(f) the connection of the device or equipment to a phone or other system that may be used to transmit information in any form and the use of the system in relation to the operation of the device or equipment; and

(g) the provision of assistance or technical expertise to the law enforcement officer primarily responsible for executing the warrant in the installation, use, maintenance or retrieval of the device or equipment.

(4) A surveillance device warrant may authorise 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 surveillance device or enhancement equipment under the warrant.

(5) The authority conferred under a warrant may be exercised by a law enforcement officer acting in the performance of the officer's duty.

(6) In addition, the authority conferred under a warrant for the use of a surveillance device may be exercised by an authorised person acting in the performance of the authorised person's duty.

(7) This section applies to a warrant subject to any conditions stated in the warrant.

(8) A surveillance device warrant may authorise the installation or use of a surveillance device outside this jurisdiction only if the offence for which it is sought is a relevant offence.

(9) This section does not authorise the doing of anything for which a warrant would be required under the *Telecommunications (Interception) Act 1979* (Cth).

24. Extension and variation of warrant

(1) A law enforcement officer to whom a surveillance device warrant has been issued (or another person on the officer's behalf) may, at any time before the expiry of the warrant, apply:

(a) for an extension of the warrant for a period not exceeding 90 days from the day on which it would otherwise expire; or

(b) for a variation of any of the other terms of the warrant.

(2) The application must be made to:

(a) a Judge if the warrant was issued by a Judge; or

(b) a magistrate if the warrant was issued by a magistrate.

(3) Sections 19 and 20 apply (with the necessary changes) to the application as if it were an application for the warrant.

(4) The Judge or magistrate may grant the application, subject to the conditions the Judge or magistrate considers appropriate, if satisfied the matters mentioned in section 21(1) still exist having regard to the matters mentioned in section 21(2).

(5) If the Judge or magistrate grants the application, the Judge or magistrate must endorse the new expiry date or the other varied term on the original warrant.

(6) An application may be made under this section more than once.

25. Revocation of warrant

(1) A surveillance device warrant may be revoked at any time before the expiration of the period of validity stated in it by:

(a) a Judge if a Judge issued the warrant; or

(b) a magistrate if a magistrate issued the warrant.

(2) A Judge or magistrate may revoke a surveillance device warrant:

(a) after receiving a report under section 58 in relation to the warrant; or

(b) on application by or on behalf of a law enforcement officer.

(3) An application for the revocation of a warrant must not be heard in open court.

(4) A Judge or magistrate who revokes a warrant must give notice of the revocation to the chief officer of the relevant law enforcement agency.

(5) If the Judge or magistrate revokes the warrant on the application of a law enforcement officer, the Judge or magistrate is taken to have given notice of the revocation to the chief officer under subsection (4) when the Judge or magistrate revokes the warrant.

26. Discontinuing use of surveillance device under warrant

(1) This section applies if a surveillance device warrant is issued to a law enforcement officer of a law enforcement agency.

(2) If the chief officer of the law enforcement agency is satisfied the use of a surveillance device under the warrant is no longer necessary for the purpose of enabling evidence to be obtained of the commission of the offence or the identity or location of the offender, the chief officer must:

(a) take the steps necessary to ensure use of the surveillance device authorised by the warrant is discontinued as soon as practicable; and

(b) ensure an application is made for the revocation of the warrant.

(3) If the chief officer is given notice the warrant has been revoked by a Judge or magistrate, the chief officer must take the steps necessary to ensure use of the surveillance device authorised by the warrant is discontinued immediately.

(4) If the law enforcement officer to whom the warrant is issued, or who is primarily responsible for executing the warrant, reasonably believes use of

a surveillance device under the warrant is no longer necessary for the purpose of enabling evidence to be obtained of the commission of the offence or the identity or location of the offender, the officer must tell the chief officer of the law enforcement agency as soon as practicable.

Division 3 – Retrieval Warrants

27. Application for retrieval warrant

(1) A law enforcement officer (or another person on the officer's behalf) may apply for the issue of a retrieval warrant for a surveillance device if:

(a) the device was lawfully installed on a place or thing; and

(b) the law enforcement officer reasonably believes the device is still on the place or thing or on another place or thing.

(2) The application may be made to:

(a) a Judge in any case; or

(b) a magistrate in the case of an application for a retrieval warrant authorising the retrieval of a tracking device only.

(3) The application must be supported by an affidavit stating the grounds on which the warrant is sought.

(4) However, the application may be made before an affidavit is prepared or sworn if the applicant reasonably believes:

(a) the immediate retrieval of a surveillance device is necessary; and

(b) it is impracticable for an affidavit to be prepared or sworn before an application for a warrant is made.

(5) If subsection (4) applies, the applicant must:

(a) give as much information as the Judge or magistrate considers is reasonably practicable in the circumstances; and

(b) not later than the day following the making of the application, send a duly sworn affidavit to the Judge or magistrate who decided the application, regardless of whether a warrant is issued.

(6) An application for a warrant must not be heard in open court.

28. Remote application

(1) If a law enforcement officer reasonably believes it is impracticable for an application for a retrieval warrant to be made in person, the application

may be made under section 27 by phone, fax, email or another form of communication.

(2) Subsection (3) applies if:

(a) an affidavit has been prepared (whether sworn or unsworn); and

(b) when making the application, the applicant has access to a fax or email facility.

(3) The applicant must fax or email a copy of the affidavit with the application to the Judge or magistrate who is to decide the application.

29. Deciding application

(1) A Judge or magistrate may issue a retrieval warrant if satisfied:

(a) there are reasonable grounds for the belief founding the application for the warrant; and

(b) in the case of an unsworn application – it would have been impracticable for an affidavit to have been prepared or sworn before the application was made; and

(c) in the case of a remote application – it would have been impracticable for the application to have been made in person.

(2) In deciding whether a retrieval warrant should be issued, the Judge or magistrate must have regard to:

(a) the extent to which anyone's privacy is likely to be affected; and

(b) the public interest in retrieving the device sought to be retrieved.

30. What retrieval warrant must contain

(1) A retrieval warrant must:

(a) state the Judge or magistrate is satisfied of the matters mentioned in section 29(1) and has had regard to the matters mentioned in section 29(2); and

(b) state:

(i) the name of the applicant; and

(ii) the date the warrant is issued; and

(iii) the kind of surveillance device authorised to be retrieved; and

(iv) the place or thing from which the device is to be retrieved; and

(v) the period (not exceeding 90 days) during which the warrant is in force; and

(vi) the name of the law enforcement officer primarily responsible for executing the warrant; and

(vii) any conditions subject to which a place may be entered under the warrant; and

(viii) the time within which a report for the warrant must be made to the Judge or magistrate under section 58.

(2) A warrant must be signed by the issuing Judge or magistrate and include the name of the Judge or magistrate.

(3) If the Judge or magistrate issues the warrant on a remote application, the Judge or magistrate must:

(a) tell the applicant of:

(i) the terms of the warrant; and

(ii) the date and time of its issue; and

(b) enter the details mentioned in paragraph (a) in a register kept by the Judge or magistrate for the purpose; and

(c) give the applicant a copy of the warrant as soon as practicable.

31. What retrieval warrant authorises

(1) A retrieval warrant (subject to any conditions stated in it) authorises:

(a) the retrieval of the surveillance device stated in the warrant and any enhancement equipment relating to the device; and

(b) the entry, by force if necessary, onto the place where the device is reasonably believed to be, or another place adjoining or providing access to the place, to retrieve the device and equipment; and

(c) the breaking open of anything to retrieve the device and equipment; and

(d) if the device or equipment is installed on a thing, the temporary removal of the thing from any place where it is situated to retrieve the device and equipment and return the thing to the place; and

(e) the provision of assistance or technical expertise to the law enforcement officer primarily responsible for executing the warrant in the retrieval of the device or equipment.

(2) If the retrieval warrant authorises the retrieval of a tracking device, the warrant also authorises the use of the tracking device and any enhancement equipment relating to the device solely to locate and retrieve the device or equipment.

(3) A retrieval warrant may authorise the doing of anything reasonably necessary to conceal the fact that anything has been done in relation to the retrieval of a surveillance device or enhancement equipment under the warrant.

32. Revocation of retrieval warrant

(1) A retrieval warrant may be revoked at any time before the expiration of the period of validity stated in it by:

(a) a Judge if a Judge issued the warrant; or

(b) a magistrate if a magistrate issued the warrant.

(2) A Judge or magistrate may revoke a retrieval warrant:

(a) after receiving a report under section 58 in relation to the warrant; or

(b) on application by or on behalf of a law enforcement officer.

(3) An application for the revocation of a warrant must not be heard in open court.

(4) A Judge or magistrate who revokes a warrant must give notice of the revocation to the chief officer of the relevant law enforcement agency.

(5) If the Judge or magistrate revokes the warrant on the application of a law enforcement officer, the Judge or magistrate is taken to have given notice of the revocation to the chief officer under subsection (4) when the Judge or magistrate revokes the warrant.

(6) If the chief officer of a law enforcement agency is satisfied the grounds for issue of a retrieval warrant to a law enforcement officer of the agency no longer exist, the chief officer must ensure an application is made to revoke the warrant.

(7) If the law enforcement officer to whom a retrieval warrant has been issued, or who is primarily responsible for executing a retrieval warrant, reasonably believes the grounds for issue of the warrant no longer exist, the

officer must tell the chief officer of the law enforcement agency as soon as practicable.

PART 5 – EMERGENCY AUTHORISATIONS

33. When application may be made for emergency authorisation

(1) A law enforcement officer of a law enforcement agency may apply to a senior officer of the agency for an emergency authorisation for the use of a surveillance device if the law enforcement officer reasonably believes:

(a) an imminent threat of serious violence to a person or substantial damage to property exists; and

(b) the use of a surveillance device is immediately necessary for the purpose of dealing with that threat; and

(c) the circumstances are so serious and the matter is of such urgency that the use of a surveillance device is warranted; and

(d) it is not practicable in the circumstances to apply for a surveillance device warrant.

(2) In addition, a law enforcement officer of a law enforcement agency may apply to a senior officer of the agency for an emergency authorisation for the use of a surveillance device if:

(a) a serious drug offence or an offence against a law of another jurisdiction or the Commonwealth that corresponds to a serious drug offence has been, is being, is about to be or is likely to be committed; and

(b) the use of a surveillance device is immediately necessary for:

(i) an investigation into the offence; or

(ii) enabling evidence or information to be obtained of the commission of the offence or the identity or location of the offender; and

(c) the circumstances are so serious and the matter is of such urgency that the use of a surveillance device is warranted; and

(d) it is not practicable in the circumstances to apply for a surveillance device warrant.

34. How application is made

An application for an emergency authorisation may be made orally, in writing or by phone, fax, email or another form of communication.

35. When authorisation may be given

A senior officer may give an emergency authorisation for the use of a surveillance device on a properly made application if satisfied there are reasonable grounds for the belief founding the application.

36. Effect of authorisation

(1) An emergency authorisation may authorise the law enforcement officer to whom it is given to do anything that a surveillance device warrant may authorise law enforcement officers to do.

(2) However, an emergency authorisation (serious drugs offence) cannot authorise the installation or use of a surveillance device outside this jurisdiction.

37. Application for approval after use of surveillance device under emergency authorisation

(1) Within 2 business days after giving an emergency authorisation, a senior officer (or another person on the officer's behalf) must apply to a Judge for approval of the exercise of powers under the emergency authorisation.

(2) The application must:

(a) state:

(i) the name of the applicant; and

(ii) the kind of surveillance device sought to be approved and, if a warrant is sought, the nature and duration of the warrant; and

(b) be supported by an affidavit stating the grounds on which the approval (and warrant, if any) is sought.

(3) The Judge may refuse to consider the application until the applicant gives the Judge all the information the Judge requires about the application in the way the Judge requires.

(4) The application must not be heard in open court.

38. Consideration of application

(1) In deciding an application for approval for an emergency authorisation (serious violence), the Judge must consider the following matters:

(a) the nature of the risk of serious violence to a person or substantial damage to property;

(b) the extent to which issuing a surveillance device warrant would have helped reduce or avoid the risk;

(c) the extent to which law enforcement officers could have used alternative methods of investigation to help reduce or avoid the risk;

(d) how much the use of alternative methods of investigation could have helped reduce or avoid the risk;

(e) how much the use of alternative methods of investigation would have prejudiced the safety of the person or property because of delay or for another reason;

(f) whether or not it was practicable in the circumstances to apply for a surveillance device warrant.

(2) In deciding an application for approval for an emergency authorisation (serious drugs offence), the Judge must consider the following matters:

(a) the nature of the serious and urgent circumstances for which the emergency authorisation was sought;

(b) the extent to which law enforcement officers could have used alternative methods of investigation;

(c) whether or not it was practicable in the circumstances to apply for a surveillance device warrant.

(3) In considering matters, the Judge must be mindful of the intrusive nature of using a surveillance device.

(4) Subsections (1) and (2) do not limit the matters the Judge may consider in deciding the application.

39. Judge may approve emergency use of powers

(1) After considering an application for approval for an emergency authorisation (serious violence), the Judge may approve the application if satisfied there were reasonable grounds to believe:

(a) there was a risk of serious violence to a person or substantial damage to property; and

(b) using a surveillance device may have helped reduce the risk; and

(c) it was not practicable in the circumstances to apply for a surveillance device warrant.

(2) After considering an application for approval for an emergency authorisation (serious drugs offence), the Judge may approve the application if satisfied:

(a) the circumstances of the case were serious and urgent; and

(b) using a surveillance device may have helped to obtain evidence or information of the commission of the offence or the identity or location of the offender; and

(c) it was not practicable in the circumstances to apply for a surveillance device warrant.

(3) If the Judge approves the application, the Judge may issue a surveillance device warrant for the continued use of the surveillance device as if the application were an application for a surveillance device warrant under Part 4, Division 2.

(4) If the Judge does not approve the application, the Judge may:

(a) order the use of the surveillance device cease; and

(b) authorise, subject to any conditions the Judge considers appropriate, the retrieval of the device.

(5) In any case, the Judge may order any information obtained from or relating to the exercise of powers under the emergency authorisation or any record of the information be dealt with in the way stated in the order.

40. Admissibility of evidence

If the Judge approves the exercise of powers under the emergency authorisation, evidence obtained because of the exercise of the powers is not inadmissible in any proceeding only because the evidence was obtained before the approval.

PART 6 – EMERGENCY USE OF LISTENING AND OPTICAL SURVEILLANCE DEVICES IN PUBLIC INTEREST

Division 1 – Preliminary matters

41. Definition

In this Division:

"public interest" includes the interests of national security, public safety, the economic well-being of Australia, the protection of public health and morals and the protection of the rights and freedoms of citizens.

42. Unlawful acts

This Part does not apply if, in the course of installing or using a listening device or optical surveillance device, an act is done that is unlawful under any law other than this Act.

Division 2 – Emergency use of listening and optical surveillance devices in public interest

43. Emergency use of listening device in public interest

A person may use a listening device to listen to, monitor or record a private conversation if at the time of use there are reasonable grounds for believing the circumstances are so serious and the matter is of such urgency that the use of the device is in the public interest.

44. Emergency use of optical surveillance device in public interest

A person may use an optical surveillance device to record visually or observe a private activity if at the time of use there are reasonable grounds for believing the circumstances are so serious and the matter is of such urgency that the use of the device is in the public interest.

45. Report to Judge

(1) A person is guilty of an offence if the person:

(a) uses a listening device or optical surveillance device under section 43 or 44; and

(b) does not give a written report complying with subsection (2) to a Judge within 2 business days after starting to use the device.

Maximum penalty: 100 penalty units or imprisonment for 1 year.

(2) The report must state the following:

(a) particulars of the device used;

(b) particulars of the use of the device and the period during which it was used;

(c) the name, if known, of any person whose private conversation was listened to, monitored or recorded or whose private activity was observed or visually recorded;

(d) the circumstances that caused the person to believe it was necessary to listen to, monitor or record the private conversation or observe or visually record the private activity;

(e) the general use made or to be made of any evidence or information obtained by use of the device.

(3) The Judge may direct any record of evidence or information obtained by the use of the device to which the report relates be brought before the Judge.

(4) A record of the evidence or information brought before the Judge must be kept in the custody of the Supreme Court.

(5) The Judge may order the record or information be returned, made available to any person or destroyed.

Division 3 – Publication and communication of information

46. Order allowing publication or communication in public interest

(1) On application made under section 47, a Judge may make an order that a person may publish or communicate any of the following that has come to the person's knowledge as a direct or indirect result of the use of a surveillance device under Division 2:

(a) a private conversation;

(b) a report or record of a private conversation;

(c) a record of a private activity.

(2) However, the Judge may make the order only if satisfied the publication or communication should be made to protect or further the public interest.

(3) The Judge may make the order subject to the conditions the Judge considers necessary in the circumstances.

(4) On application made under section 47, a Judge may make an order that a report or record of a private conversation or a record of a private activity obtained as a direct or indirect result of the use of a surveillance device under Division 2:

(a) be made available to any person or destroyed; or

(b) be given to: or

(i) the Territory Police Force or police force of a State or another Territory;

(ii) the Australian Federal Police; or

(iii) the Australian Crime Commission; or

(c) be kept in the custody of the Supreme Court if the Judge is satisfied it is necessary to protect or further the public interest.

47. Application for publication order

(1) An application for an order under section 46 must:

(a) be in writing; and

(b) state the grounds on which it is made; and

(c) include an affidavit of the applicant deposing to the facts required by the Judge to enable the Judge to deal with the application.

(2) Unless the applicant is a law enforcement officer, the Judge may require the applicant to give notice of the application to the person the Judge considers appropriate.

(3) The Judge may require further information to be given, orally or by affidavit, in relation to the application.

48. Confidentiality

(1) An application under this Part must not be heard in open court.

(2) The following material must not be made available by the Supreme Court for search by any person except on the direction of a Judge:

(a) an application under this Part and any material relating to it, including any record of it or of the hearing of it;

(b) an order made on an application under this Part;

(c) a written report given to a Judge under section 45;

(d) any record of evidence or information brought before a Judge under section 45(3).

PART 7 – RECOGNITION OF CORRESPONDING WARRANTS AND AUTHORISATIONS

49. Corresponding warrants

A corresponding warrant may be executed in this jurisdiction in accordance with its terms as if it were a surveillance device warrant or retrieval warrant issued under Part 4, Division 2 or 3.

50. Corresponding emergency authorisations

(1) A corresponding emergency authorisation authorises the use of a surveillance device in accordance with its terms in this jurisdiction as if it were an emergency authorisation given under Part 5.

(2) Subsection (1) does not apply at any time after a Judge orders, under a provision of a corresponding law that corresponds to section 39(4), the use of a surveillance device under the corresponding emergency authorisation cease.

PART 8 – COMPLIANCE AND MONITORING

Division 1 – Restrictions on use, communication and publication of information

51. Protected information

(1) Protected information is local protected information or corresponding protected information.

(2) Local protected information is:

(a) any information obtained from the use of a surveillance device under a warrant or emergency authorisation; or

(b) any information relating to:

(i) an application for, issue of, existence of or expiry of a warrant or emergency authorisation; or

(ii) an application for approval of powers exercised under an emergency authorisation.

(3) Corresponding protected information is:

(a) any information obtained from the use of a surveillance device under a corresponding warrant or corresponding emergency authorisation; or

(b) any information relating to:

(i) an application for, issue of, existence of or expiry of a corresponding warrant or corresponding emergency authorisation; or

(ii) an application under a corresponding law for approval of powers exercised under a corresponding emergency authorisation.

52. Prohibition on use, communication or publication of protected information

(1) A person is guilty of an offence if:

(a) the person uses, communicates or publishes any information; and

(b) the information is protected information; and

(c) the use, communication or publication of the information is not permitted by this Division.

Maximum penalty: 250 penalty units or imprisonment for 2 years.

(2) A person is guilty of an offence if:

(a) the person uses, communicates or publishes any information; and

(b) the information is protected information; and

(c) the use, communication or publication of the information is not permitted by this Division; and

(d) the use, communication or publication of the information:

(i) endangers the health or safety of any person; or

(ii) prejudices the effective conduct of an investigation into an offence.

Maximum penalty: 2 000 penalty units or imprisonment for 10 years.

(3) Subsections (1) and (2) do not apply to:

(a) the use, communication or publication of:

(i) any information that has been disclosed in a proceeding in open court; or

(ii) any information that has entered the public domain; or

(b) the use or communication of protected information by a person who reasonably believes the use or communication is necessary to help prevent or reduce the risk of serious violence to a person or substantial damage to property; or

(c) the communication to the Director-General (as defined in the *Australian Security Intelligence Organisation Act 1979* (Cth)) of protected information that relates or appears to relate to activities prejudicial to security as defined in that Act; or

(d) the use or communication of information mentioned in paragraph (c) by an officer of the Australian Security Intelligence Organisation in the performance of the officer's official functions; or

(e) the use or communication of information to a foreign country or appropriate authority of a foreign country under the *Mutual Assistance in Criminal Matters Act 1987* (Cth).

(4) Subsection (3)(c) and (d) do not authorise the use, communication or publication of protected information in relation to an emergency authorisation or corresponding emergency authorisation unless the use of powers under the authorisation has been approved under section 39 or a corresponding provision of a corresponding law.

53. Permitted use of local protected information

(1) Local protected information may be used, communicated or published if it is necessary to do so for any of the following purposes:

(a) the investigation of an offence;

(b) the making of a decision whether or not to bring a relevant proceeding for an offence;

(c) a relevant proceeding for an offence;

(d) an investigation of a complaint against, or the conduct of, a public officer under this Act or a corresponding law;

(e) the making of a decision in relation to the appointment, re-appointment, term of appointment, termination or retirement of a person mentioned in paragraph (d);

(f) the keeping of records and the making of reports by a law enforcement agency under Division 2;

(g) an inspection by the Commonwealth Ombudsman under a provision of a corresponding law that corresponds to section 63 or 65;

(h) an investigation of a complaint under the *Information Act* or a law of a participating jurisdiction or the Commonwealth about the privacy of personal information.

(2) Subsection (1)(a), (b) and (c) do not authorise the use, communication or publication of protected information in relation to an emergency authorisation unless the use of powers under the authorisation has been approved under section 39.

(3) A reference in subsection (1) to an offence (whether of this jurisdiction or another jurisdiction) is a reference to an offence, whether or not the offence for which the relevant warrant or emergency authorisation was issued or given.

54. Permitted use of corresponding protected information

(1) Corresponding protected information may be used, communicated or published if it is necessary to do so for any of the following purposes:

(a) the investigation of a relevant offence within the meaning of this Act or a corresponding law;

(b) the making of a decision whether or not to bring:

(i) a relevant proceeding for a relevant offence; or

(ii) a relevant proceeding under a corresponding law for a relevant offence under that law;

(c) a relevant proceeding for a relevant offence or a relevant proceeding under a corresponding law for a relevant offence under that law;

(d) an investigation of a complaint against, or the conduct of, a public officer under this Act or a corresponding law;

(e) the making of a decision in relation to the appointment, re-appointment, term of appointment, termination or retirement of a person mentioned in paragraph (d);

(f) the keeping of records and the making of reports by a law enforcement agency under a corresponding law under a provision of the corresponding law that corresponds to Division 2;

(g) an inspection under a provision of a corresponding law that corresponds to section 63;

(h) an investigation of a complaint under the *Information Act* or a law of a participating jurisdiction or of the Commonwealth about the privacy of personal information.

(2) Subsection (1)(a), (b) and (c) do not authorise the use, communication or publication of protected information in relation to a corresponding emergency authorisation unless the use of powers under that authorisation has been approved under a provision of a corresponding law that corresponds to section 39.

(3) A reference in subsection (1) to a relevant offence (whether of this jurisdiction or another jurisdiction) is a reference to a relevant offence, whether or not the offence for which the relevant corresponding warrant or emergency authorisation was issued or given.

55. Dealing with records obtained by use of surveillance devices

(1) The chief officer of a law enforcement agency must ensure:

(a) a record or report obtained by the use of a surveillance device by a law enforcement officer of the agency under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation is kept in a secure place that is not accessible to people who are not entitled to deal with the record or report; and

(b) a record or report mentioned in paragraph (a) is destroyed, if satisfied it is not likely to be required in relation to a purpose mentioned in section 52(3), 53(1) or 54(1).

(2) Subsection (1) does not apply to a record or report received in evidence in a legal or disciplinary proceeding.

56. Protection of surveillance device technologies and methods

(1) In any proceeding, a person may object to the disclosure of information on the ground the information, if disclosed, could reasonably be expected to reveal details of surveillance device technology or methods of installation, use or retrieval of surveillance devices.

(2) If the person conducting or presiding over the proceeding (the "presiding officer") is satisfied the ground of objection is made out, the presiding officer may order the person who has the information not be required to disclose it in the proceeding.

(3) In deciding whether or not to make the order, the presiding officer must take into account whether disclosure of the information:

(a) is necessary for the fair trial of the defendant; or

(b) is in the public interest.

(4) Subsection (2) does not affect a provision of another law under which a law enforcement officer cannot be compelled to disclose information or make statements in relation to the information.

(5) If the presiding officer is satisfied publication of any information disclosed in the proceeding could reasonably be expected to reveal details of surveillance device technology or methods of installation, use or retrieval of surveillance devices, the presiding officer must make the orders prohibiting or restricting publication of the information the presiding officer considers necessary to ensure the details are not revealed.

(6) Subsection (5) does not apply to the extent the presiding officer considers the interests of justice require otherwise.

(7) In this section:

"proceeding" includes a proceeding before:

(a) a court or tribunal; and

(b) a board of inquiry under the *Inquiries Act*.

57. Protected information in custody of court

A person is not entitled to search any protected information in the custody of a court unless the court otherwise orders in the interests of justice.

Division 2 – Reporting and record-keeping

58. Report to Judge or magistrate

(1) A law enforcement officer to whom a warrant is issued, or who is primarily responsible for executing a warrant issued, under this Act must, within the time stated in the warrant, make a report under this section to the Judge or magistrate who issued the warrant.

(2) For a surveillance device warrant, the report must:

(a) state whether the warrant was executed; and

(b) if the warrant was executed:

(i) state the kind of surveillance device used; and

(ii) state the period during which the device was used; and

(iii) state the name, if known, of any person whose conversations or activities were overheard, listened to, monitored, recorded or observed by the use of the device; and

(iv) state the name, if known, of any person whose geographical location was determined by the use of the device; and

(v) give details of any place on which the device was installed or used; and

(vi) give details of anything on which the device was installed or any place where the thing was located when the device was installed; and

(vii) give details of the benefit to the investigation of the use of the device and of the general use made or to be made of any evidence or information obtained by the use of the device; and

(viii) give details of the compliance with the conditions (if any) to which the warrant was subject; and

(c) if the warrant was extended or varied, state:

(i) the number of extensions or variations; and

(ii) the reasons for the extensions or variations.

(3) For a retrieval warrant, the report must:

(a) give details of any place entered, anything opened and anything removed and replaced under the warrant; and

(b) state whether the surveillance device was retrieved under the warrant; and

(c) if the device was not retrieved, state the reason why; and

(d) give details of the compliance with the conditions (if any) to which the warrant was subject.

(4) On receiving the report, the Judge or magistrate may order that any information obtained from or relating to the execution of the warrant, or any record of the information, be dealt with in the way stated in the order.

59. Annual reports

(1) The chief officer of a law enforcement agency must give a report to the Minister that includes the following information for each financial year:

(a) the number of applications for warrants by and the number of warrants issued to law enforcement officers of the agency during the year;

(b) the number of applications for emergency authorisations by and the number of emergency authorisations given to law enforcement officers of the agency during the year;

(c) the number of remote applications for warrants by law enforcement officers of the agency during the year;

(d) the number of applications for warrants or emergency authorisations by law enforcement officers of the agency that were refused during the year, and the reasons for refusal;

(e) the number of applications for extensions of warrants by law enforcement officers of the agency during the year, the number of extensions granted or refused and the reasons why they were granted or refused;

(f) the number of arrests made by law enforcement officers of the agency during the year on the basis (wholly or partly) of information obtained by the use of a surveillance device under a warrant or emergency authorisation;

(g) the number of prosecutions that were started in this jurisdiction during the year in which information obtained by the use of a surveillance device under a warrant or emergency authorisation was given in evidence and the number of the prosecutions in which a person was found guilty;

(h) any other information relating to the use of surveillance devices and the administration of this Act the Minister considers appropriate.

(2) The information mentioned in subsection (1)(a) and (b) must be presented in a way that shows the number of warrants issued and emergency authorisations given for each different kind of surveillance device.

(3) The report must be given to the Minister within 3 months after the end of the financial year.

(4) The Minister must, within 7 sitting days after receiving the report, table a copy of it in the Legislative Assembly.

60. Keeping documents for warrants and emergency authorisations

The chief officer of a law enforcement agency must keep the following documents:

(a) each warrant issued to a law enforcement officer of the agency;

(b) each notice given to the chief officer under section 25(4) of revocation of a warrant;

(c) each emergency authorisation given to a law enforcement officer of the agency;

(d) each application made by a law enforcement officer of the agency for an emergency authorisation;

(e) a copy of each application made by a law enforcement officer of the agency for:

(i) a warrant; and

(ii) an extension, variation or revocation of a warrant; and

(iii) approval of the exercise of powers under an emergency authorisation;

(f) a copy of each report made to a Judge or magistrate under section 58;

(g) a copy of each certificate issued by a senior officer of the agency under section 71.

61. Other records to be kept

The chief officer of a law enforcement agency must keep the following records:

(a) a statement as to whether each application made by a law enforcement officer of the agency for a warrant, or extension, variation or revocation of a warrant, was granted, refused or withdrawn;

(b) a statement as to whether each application made by a law enforcement officer of the agency for an emergency authorisation, or for approval of powers exercised under an emergency authorisation, was granted, refused or withdrawn;

(c) details of each use by the agency, or by a law enforcement officer of the agency, of information obtained by the use of a surveillance device by a law enforcement officer of the agency;

(d) details of each communication by a law enforcement officer of the agency to a person other than a law enforcement officer of the agency of information obtained by the use of a surveillance device by a law enforcement officer of the agency;

(e) details of each occasion when, to the knowledge of a law enforcement officer of the agency, information obtained by the use of a surveillance device by a law enforcement officer of the agency was given in evidence in a relevant proceeding;

(f) details of the destruction of records or reports under section 55(1)(b).

62. Register of warrants and emergency authorisations

(1) The chief officer of a law enforcement agency must keep a register of warrants and emergency authorisations.

(2) The register must, for each warrant issued to a law enforcement officer of the agency, state the following:

(a) the date of issue;

(b) the name of the Judge or magistrate who issued it;

(c) the name of the law enforcement officer primarily responsible for executing it;

(d) the offence for which it was issued;

(e) the period during which it is in force;

(f) details of any extension or variation of it.

(3) The register must, for each emergency authorisation given to a law enforcement officer of the agency, state the following:

(a) the date it was given;

(b) the name of the senior officer who gave it;

(c) the name of the law enforcement officer to whom it was given;

(d) the offence for which it was given;

(e) the date on which the application for approval of powers exercised under it was made.

Division 3 – Inspections

63. Inspection of records by Ombudsman

(1) The Ombudsman must, from time to time, inspect the records of a law enforcement agency to decide the extent of compliance with this Act by the agency and law enforcement officers of the agency.

(2) For the inspection, the Ombudsman:

(a) after notifying the chief officer of the agency, may enter at any reasonable time a place occupied by the agency; and

(b) is entitled to have full and free access at all reasonable times to all records of the agency that are relevant to the inspection; and

(c) may require a member of staff of the agency to give the Ombudsman information that:

(i) is in the member's possession or to which the member has access; and

(ii) is relevant to the inspection.

(3) The chief officer must ensure members of staff of the agency give the Ombudsman any assistance the Ombudsman reasonably requires to enable the Ombudsman to perform functions under this section.

64. Ombudsman's reports on investigations

(1) The Ombudsman must make a written report to the Minister at 6-monthly intervals on the results of each inspection under section 63.

(2) The Minister must, within 7 sitting days after receiving a report, table a copy of it in the Legislative Assembly.

65. Commonwealth Ombudsman's reports on investigations

The Minister must, within 7 sitting days after receiving a report by the Commonwealth Ombudsman under section 61(3) of the *Surveillance Devices Act 2004* (Cth), table a copy of it in the Legislative Assembly.

PART 9 – FURTHER OFFENCES, ENFORCEMENT AND LEGAL PROCEEDINGS

Division 1 – Offences

66. Possession of surveillance device for unlawful use

A person must not possess a surveillance device knowing it is intended for use in contravention of this Act or a law of the Commonwealth or another jurisdiction.

Maximum penalty: 250 penalty units or imprisonment for 2 years.

67. Damaging etc. surveillance device

(1) A person is guilty of an offence if:

(a) the person:

(i) engages in conduct that causes damage to, or interferes with the use of, a surveillance device installed on a place or thing; or

(ii) removes or retrieves a surveillance device installed on a place or thing; and

(b) a law enforcement officer lawfully installed the device.

Maximum penalty: 250 penalty units or imprisonment for 2 years.

(2) Subsection (1) does not apply if the person is authorised to damage, interfere with, remove or retrieve the device by or under this Act or a law of the Commonwealth or another jurisdiction.

Division 2 – Search and seizure of surveillance devices

68. Power to search and seize

(1) A police officer who reasonably believes a person possesses a surveillance device that is intended to be used in contravention of this Act, a law of the Commonwealth or another jurisdiction may:

(a) stop and search the person; or

(b) stop, detain and search a vehicle the officer reasonably believes may contain the device or evidence concerning the possession or intended use of the device; or

(c) at any time, enter and search a place the officer reasonably believes the device is being kept or may contain evidence of the possession or intended use of the device.

(2) If the police officer reasonably believes a surveillance device has been, is being, is about to be or is likely to be used in connection with the commission of an offence, the officer may seize and remove the device and any connection device.

(3) The police officer may exercise a power under this section with the help, and using the force, that is reasonable in the circumstances.

(4) In this section:

"search", of a person, means a search of the person or things in the person's possession, that may include:

(a) requiring the person to remove only the person's overcoat, coat or jacket or similar article of clothing and any gloves, shoes and hat; and

(b) an examination of the things.

69. Retention of seized device

(1) This section applies if a police officer seizes a surveillance device or connection device under section 68(2).

(2) The seized device may be retained until the final decision on a proceeding in relation to the device unless it is ordered to be returned or otherwise dealt with under subsection (4).

(3) A person claiming to have an interest (whether as owner or otherwise) in the device may apply to a magistrate for its return or for it to be otherwise dealt with.

(4) The magistrate may make the order the magistrate considers just:

(a) for the release of or other dealing with the device subject to any conditions relating to its production as evidence at a proceeding; or

(b) for the retention of the device by the Commissioner of Police.

Division 3 – Legal proceedings

70. Admissibility in criminal proceeding of information inadvertently obtained

(1) This section applies if a private conversation or private activity has inadvertently come to the knowledge of a law enforcement officer or authorised person as a direct or indirect result of the use of a surveillance device under a surveillance device warrant or emergency authorisation.

(2) In a criminal proceeding, the law enforcement officer or authorised person may:

(a) give evidence of the conversation or activity; or

(b) give evidence obtained as a consequence of the conversation or activity coming to the person's knowledge.

(3) Subsection (2) applies regardless of whether the warrant or authorisation was issued for a purpose that allowed the evidence to be obtained.

(4) However, the evidence is inadmissible if the court is satisfied the application on which the warrant or authorisation was issued was not made in good faith.

71. Evidentiary certificates

(1) A senior officer of a law enforcement agency, or a person assisting the senior officer, may issue a written certificate signed by the officer or person stating any facts the officer or person considers relevant in relation to:

(a) anything done by a law enforcement officer of the agency, or by a person assisting or providing technical expertise to the officer, in relation to the execution of a warrant or under an emergency authorisation; or

(b) anything done by a law enforcement officer of the agency in relation to:

(i) the communication by a person to another person of relevant information; or

(ii) the making use of relevant information; or

(iii) the making of a record of relevant information; or

(iv) the custody of a record of relevant information.

(2) For subsection (1)(b), relevant information is information obtained by the use of a surveillance device under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation.

(3) A document purporting to be a certificate issued under subsection (1) or a corresponding provision of a corresponding law is admissible in evidence in any proceeding.

(4) Subsection (3) does not apply to a certificate to the extent the certificate states facts in relation to anything done under an emergency authorisation or corresponding emergency authorisation unless the use of powers under the authorisation has been approved under section 39 or a corresponding provision of a corresponding law.

72. Liability of executive officers of body corporate

(1) If a body corporate commits an offence against this Act (the "principal offence"), each of the executive officers of the body corporate commits an offence (the "secondary offence") and is liable to the penalty applicable to an individual who commits the principal offence.

(2) However, it is a defence for an executive officer to establish:

(a) the officer did not know, and could not reasonably have been expected to know, the principal offence was to be or was being committed; or

(b) the officer exercised due diligence to prevent the commission of the principal offence.

(3) The executive officer may be found guilty of the secondary offence even though the body corporate has not been charged with, or found guilty of, the principal offence.

(4) This section does not affect the liability of the body corporate for the principal offence.

(5) In this section:

"executive officer", of a body corporate, means a director or other person who is concerned with, or takes part in, the management of the body corporate, and includes a constituent member of a body corporate incorporated for a public purpose by a law of the Commonwealth or a State or Territory.

73. Forfeiture orders

(1) If a person (the "offender") is found guilty of an offence against this Act, the court may make either or both of the following orders (each a "forfeiture order"):

(a) an order that any surveillance device or connection device used in connection with the commission of the offence is forfeited to the Territory;

(b) an order that a report or record of information obtained by the use of a surveillance device relating to the offence is forfeited to the Territory.

(2) Before making a forfeiture order under subsection (1)(a), the court may give notice to, and hear, the persons it considers appropriate.

(3) A forfeiture order is in addition to a penalty imposed on the offender.

(4) When imposing a penalty on the offender, the court must not take into account its power to make a forfeiture order.

(5) On the making of a forfeiture order, a law enforcement officer may seize the device to which the offence relates.

(6) For seizing the device, the law enforcement officer may, with the help, and using the force, that is reasonable in the circumstances:

(a) enter a place the officer reasonably believes the device may be found; and

(b) remain on the place for as long as reasonably required to search the place.

PART 10 – MISCELLANEOUS MATTERS

74. Authorised persons

(1) The Commissioner of Police may appoint an eligible employee to be an authorised person to use a surveillance device under a warrant.

(2) An eligible employee may be appointed only if the Commissioner is satisfied the employee has the qualifications or experience to use surveillance devices.

(3) An appointment is subject to the conditions stated in the instrument of appointment.

(4) In this section:

"eligible employee" means:

(a) an Aboriginal Community Police officer or Police auxiliary appointed under section 19 of the *Police Administration Act*; or

(b) a public sector employee assigned to the Police Civil Employment Unit;

"Police Civil Employment Unit" means the Agency of that name mentioned in Schedule 1 to the *Public Sector Employment and Management Act*.

75. Acquisition on just terms

If, apart from this section, property would be acquired from a person because of the operation of this Act other than on just terms:

(a) the person is entitled to receive from the Territory the compensation necessary to ensure the acquisition is on just terms; and

(b) a court of competent jurisdiction may decide the amount of compensation or make the orders it considers necessary to ensure the acquisition is on just terms.

76. Protection from liability

(1) This section applies to a person who is or has been:

(a) a police officer; or

(b) an authorised person; or

(c) a person assisting a police officer or authorised person exercise a power or perform a function under this Act.

(2) The person is not civilly or criminally liable for an act done or omitted to be done by the person in good faith in the exercise or purported exercise of a power, or the performance or purported performance of a function, under this Act.

(3) Subsection (2) does not affect any liability the Territory would, apart from this section, have for the act or omission.

(4) Subsections (2) and (3) have effect subject to Part VIIA of the *Police Administration Act* to the extent it relates to the civil liability of a person who is or has been a police officer.

77. Regulations

(1) The Administrator may make regulations under this Act.

(2) The regulations may:

(a) prescribe fees payable under this Act; and

(b) for an offence against the regulations, prescribe a fine not exceeding 200 penalty units.

PART 11 – REPEALS AND TRANSITIONAL MATTERS

78. Repeal

The *Surveillance Devices Act* (Act No. 56 of 2000) is repealed.

79. Definitions

In this Part:

"commencement date" means the day on which section 78 commences;

"repealed Act" means the *Surveillance Devices Act* as in force immediately before the commencement date.

80. Undecided applications relating to warrants

(1) An undecided application for a warrant under section 9 of the repealed Act is taken to be an application for a surveillance device warrant or retrieval warrant.

(2) An undecided application for an amendment of the terms of a warrant under section 19 of the repealed Act is taken to be an application for the extension or variation of a surveillance device warrant or retrieval warrant.

(3) An undecided application for an extension of a warrant under section 20 of the repealed Act is taken to be an application for the extension or variation of a surveillance device warrant or retrieval warrant.

(4) In this section:

"undecided application" means an application that has not been decided immediately before the commencement date.

81. Warrants

(1) This section applies to a warrant issued under section 12 of the repealed Act and in force immediately before the commencement date.

(2) The warrant is taken to be a surveillance device warrant or retrieval warrant authorising the matters stated in it.

(3) The warrant continues in force until the date it would have expired under the repealed Act had this Act not been enacted.

82. Urgent authorisations

(1) An urgent authorisation issued under section 25 of the repealed Act is taken to be an emergency authorisation.

(2) If an application for a warrant under section 29 of the repealed Act has not been made for the emergency authorisation at the beginning of the commencement date, the authorisation is taken to have been issued on the day before the commencement date.

(3) If an application for a warrant made under section 29 of the repealed Act for the emergency authorisation has not been decided at the beginning of the commencement date, the application may be decided as if it were an application under section 38 of this Act.

83. Information, records and reports obtained under repealed Act

(1) The following information is taken to be local protected information:

(a) information obtained from the use of a surveillance device under a warrant or urgent authorisation under the repealed Act;

(b) information relating to:

(i) an application for, issue of, existence of or expiry of a warrant or urgent authorisation under the repealed Act; or

(ii) an application for approval of powers exercised under an urgent authorisation under the repealed Act.

(2) A record or report obtained by the use of a surveillance device under a warrant or urgent authorisation under the repealed Act is taken to have been obtained by the use of a surveillance device under a surveillance device warrant or emergency authorisation.

PART 12 – CONSEQUENTIAL AMENDMENTS

Division 1 – Amendment of Information Act

84. Act amended

This Division amends the *Information Act*.

85. Amendment of Schedule 1 (Secrecy provisions)

Schedule 1

insert (in alphabetical order)

Surveillance Devices Act	sections 15(1), 16(1) and 52(1) and (2)

Division 2 – Amendment of Ombudsman (Northern Territory) Act

86. Act amended

This Division amends the *Ombudsman (Northern Territory) Act*.

87. Amendment of section 12 (Delegation)

(1) Section 12(1), after "under this"

insert

or another

(2) Section 12(4)

omit

88. Amendment of section 31 (Protection of Ombudsman and staff)

(1) Section 31(1)

omit

in pursuance of this Act or of an authority given under this Act

substitute

under this or another Act

(2) Section 31(4), after "under this"

insert

or another

Division 3 – Expiry of Part

89. Expiry

This Part expires on the day after it commences.