Surveillance Devices Act 2007 No 64

[2007-64]

New South Wales

Status Information

Currency of version

Historical version for 8 December 2008 to 9 December 2008 (accessed 27 December 2024 at 16:36)

Legislation on this site is usually updated within 3 working days after a change to the legislation.

Provisions in force

The provisions displayed in this version of the legislation have all commenced.

Notes—

- **See also**
  Statute Law (Miscellaneous Provisions) Bill (No 2) 2008

Authorisation

This version of the legislation is compiled and maintained in a database of legislation by the Parliamentary Counsel's Office and published on the NSW legislation website, and is certified as the form of that legislation that is correct under section 45C of the Interpretation Act 1987.

File last modified 8 December 2008

Surveillance Devices Act 2007 No 64

New South Wales

Contents

Surveillance Devices Act 2007 No 64

New South Wales

An Act to regulate the installation, use, maintenance and retrieval of surveillance devices; to repeal the *Listening Devices Act 1984*; and for other purposes.

Part 1 Preliminary

1 Name of Act

This Act is the *Surveillance Devices Act 2007*.

2 Commencement

This Act commences on a day or days to be appointed by proclamation.

3 Relationship to other laws and matters

(1) Except where there is express provision to the contrary, this Act is not intended to affect any other law of the State that prohibits or regulates the use of surveillance devices.

Note—

For example, the *Workplace Surveillance Act 2005* contains certain requirements in relation to camera surveillance. The applicable requirements of both that Act and this Act will need to be complied with if camera surveillance is carried out.

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

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

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

(3) For the avoidance of 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.

4 Definitions

(1) 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* of the Commonwealth.

building includes any structure.

business day means a day other than a Saturday, Sunday, public holiday or bank holiday in New South Wales.

chief officer means the following:

(a) in relation to the NSW Police Force—the Commissioner of Police,

(b) in relation to the Australian Crime Commission—the Chief Executive Officer of the Australian Crime Commission,

(c) in relation to the New South Wales Crime Commission—the Commissioner for the New South Wales Crime Commission,

(d) in relation to the Independent Commission Against Corruption—the Commissioner for the Independent Commission Against Corruption,

(e) in relation to the Police Integrity Commission—the Commissioner for the Police Integrity Commission,

(f) any other person prescribed by the regulations as the chief officer in relation to a law enforcement agency.

computer means any electronic device for storing, processing or transferring information.

corresponding emergency authorisation means an authorisation in the nature of an emergency authorisation given under the provisions of a corresponding law, being an authorisation in relation to a relevant offence within the meaning of the corresponding 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 the regulations to be a corresponding law.

corresponding warrant means a warrant in the nature of a surveillance device warrant or retrieval warrant issued under the provisions of a corresponding law, being a warrant in relation to a relevant offence within the meaning of that corresponding law.

data surveillance device means any device or program capable of being used to

record or monitor the input of information into or output of information from a computer, but does not include an optical surveillance device.

device includes instrument, apparatus and equipment.

disciplinary proceeding means a proceeding of a disciplinary nature under a law of any jurisdiction or of the Commonwealth.

eligible Judge is defined in section 5.

eligible Magistrate is defined in section 5.

emergency authorisation means an emergency authorisation given under Division 4 of Part 3.

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

exercise a function includes perform a duty.

function includes a power, authority or duty.

install includes attach.

jurisdiction means a State or Territory of the Commonwealth.

law enforcement agency means the following agencies:

(a) the NSW Police Force,

(b) the New South Wales Crime Commission,

(c) the Independent Commission Against Corruption,

(d) the Police Integrity Commission,

(e) any other agency prescribed by the regulations for the purposes of this definition.

law enforcement officer means the following:

(a) in relation to the NSW Police Force—a member of the NSW Police Force,

(b) in relation to the New South Wales Crime Commission—a member of the Commission, or a member of the staff of the Commission, within the meaning of the *New South Wales Crime Commission Act 1985*,

(c) in relation to the Independent Commission Against Corruption—an officer of the Commission within the meaning of the *Independent Commission Against Corruption Act 1988*,

(d) in relation to the Police Integrity Commission—an officer of the Commission within the meaning of the *Police Integrity Commission Act 1996*,

(e) in relation to an agency prescribed for the purposes of paragraph (e) of the definition of ***law enforcement agency***—any person prescribed by the regulations as a law enforcement officer in respect of that agency for the purposes of this definition,

and includes a person who is seconded to a law enforcement agency, including (but not limited to) a member of the police force or police service or a police officer (however described) of another jurisdiction.

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

maintain, in relation to a surveillance device, includes:

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

(b) replace a faulty device.

optical surveillance device means any device capable of being used to 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 that impairment.

participating jurisdiction means a jurisdiction in which a corresponding law is in force.

party:

(a) to an activity—means a person who takes part in the activity, and

(b) to a private conversation—means a person by or to whom words are spoken in the due course of the conversation or a person who, with the consent, express or implied, of any of the persons by or to whom words are spoken in the course of the conversation, records, monitors or listens to those words.

premises includes the following:

(a) land,

(b) a building,

(c) a part of a building,

(d) any place, whether built on or not,

whether in or outside this jurisdiction.

principal party, in relation to a private conversation, means a person by or to whom words are spoken in the course of the conversation.

private conversation means any words spoken by one person to another person or to other persons in circumstances that may reasonably be taken to indicate that any of those persons desires the words to be listened to only:

(a) by themselves, or

(b) by themselves and by some other person who has the consent, express or implied, of all of those persons to do so,

but does not include a conversation made in any circumstances in which the parties to it ought reasonably to expect that it might be overheard by someone else.

protected information has the meaning given to it by section 39.

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.

record includes the following:

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

(b) a record in digital form,

(c) a documentary record prepared from a record referred to in paragraph (a) or (b).

relevant offence means:

(a) an offence against a law of this jurisdiction or of the Commonwealth or another State or Territory that may be prosecuted on indictment, or

(b) an offence against the law of this jurisdiction that is prescribed by the regulations for the purposes of this definition.

relevant proceeding means the following:

(a) the prosecution of a relevant offence,

(b) a proceeding for the confiscation, forfeiture or restraint of property or for the imposition of a pecuniary penalty in connection with a relevant offence,

(c) a proceeding for the protection of a child or intellectually impaired person,

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

(e) a disciplinary proceeding against a public officer,

(f) a coronial inquest or inquiry if, in the opinion of the coroner, the event that is the subject of the inquest or inquiry may have resulted from the commission of a relevant offence,

(g) a proceeding under section 13 of the *Mutual Assistance in Criminal Matters Act 1987* of the Commonwealth in relation to a criminal matter that concerns an offence against the laws of the foreign country that made the request resulting in the proceeding, being an offence that may be prosecuted on indictment,

(h) a proceeding for the taking of evidence under section 43 of the *Extradition Act 1988* of the Commonwealth, in so far as the proceeding relates to a relevant offence,

(i) a proceeding for the extradition of a person from another jurisdiction to this jurisdiction, in so far as the proceeding relates to a relevant offence,

(j) a proceeding under Division 1 of Part 4 of the *International War Crimes Tribunals Act 1995* of the Commonwealth,

(k) a proceeding of the International Criminal Court,

(l) a compulsory examination or public inquiry before the Independent Commission Against Corruption or an inquiry before the Inspector of the Independent Commission Against Corruption,

(m) a public or private hearing before the Police Integrity Commission or an inquiry before the Inspector of the Police Integrity Commission,

(n) a hearing before the New South Wales Crime Commission,

(o) an examination before the Australian Crime Commission.

remote application for a warrant means an application referred to in section 18 or 26.

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 Division 3 of Part 3.

senior officer means the following:

(a) in relation to the NSW Police Force:

(i) the Commissioner of Police, or

(ii) any Deputy Commissioner of Police, or

(iii) any Assistant Commissioner of Police, or

(iv) any Superintendent of Police,

(b) in relation to the New South Wales Crime Commission—the Commissioner for the New South Wales Crime Commission,

(c) in relation to the Independent Commission Against Corruption—the Commissioner for the Independent Commission Against Corruption,

(d) in relation to the Police Integrity Commission—the Commissioner for the Police Integrity Commission,

(e) in relation to any other agency prescribed by the regulations for the purposes of the definition of ***law enforcement agency***—any officer prescribed by the regulations for the purposes of this definition for that agency.

serious narcotics offence means an offence under Division 2 of Part 2 of the *Drug Misuse and Trafficking Act 1985* but does not include an offence that is declared by the regulations not to be a serious narcotics offence for the purposes of this Act.

surveillance device means:

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

(b) a device that is a combination of any 2 or more of the devices referred to in paragraph (a), or

(c) a device of a kind prescribed by the regulations.

surveillance device warrant means a warrant issued under Division 2 of Part 3 or under section 35 (3).

this jurisdiction means New South Wales.

tracking device means any electronic device capable of being used to determine or monitor the geographical location of a person or an object.

unsworn application for a warrant means an application referred to in section 17 (4) or 25 (4).

use of a surveillance device includes use of the device to record a conversation or other activity.

vehicle includes the following:

(a) an aircraft,

(b) a vessel,

(c) a part of a vehicle,

whether in or outside this jurisdiction.

warrant means surveillance device warrant or retrieval warrant.

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

Note—

Subsection (2) is intended to cover the situation where an officer of this jurisdiction is conducting or participating in an investigation wholly in another jurisdiction for the purposes of an offence against a law of this jurisdiction (eg a NSW officer is investigating a conspiracy to import drugs into NSW from Victoria, and all the evidence of the offence is in Victoria).

(3) A thing is not precluded from being a listening device within the meaning of this Act merely because it is also capable of:

(a) recording or transmitting visual images (for example a video camera), or

(b) recording or transmitting its own position.

(4) A reference in this Act to:

(a) a report of a private conversation includes a reference to a report of the substance, meaning or purport of the conversation, and

(b) a record of a private conversation includes a reference to a statement prepared from such a record.

(5) A reference in this Act to the retrieval of a surveillance device includes, in relation to a data surveillance device, a reference to the removal or erasure of the device.

(6) Notes included in this Act do not form part of this Act.

5 Eligible Judges and Magistrates

(1) In this Act:

eligible Judge means a Judge in relation to whom a consent under subsection (2) and a declaration under subsection (3) are in force.

eligible Magistrate means a Magistrate in relation to whom a consent under subsection (2) and a declaration under subsection (3) are in force.

Judge means a person who is a Judge of the Supreme Court.

(2) A Judge or Magistrate may, by instrument in writing, consent to being the subject of a declaration by the Attorney General under subsection (3).

(3) The Attorney General may, by instrument in writing, declare Judges or Magistrates in relation to whom consents are in force under subsection (2) to be eligible Judges and eligible Magistrates, respectively, for the purposes of this Act.

(4) An eligible Judge has, in relation to the exercise of a function conferred on an eligible Judge by this Act, the same protection and immunity as a Judge of the Supreme Court has in relation to proceedings in the Supreme Court.

(5) An eligible Magistrate has, in relation to the exercise of a function conferred on an eligible Magistrate by this Act, the same protection and immunity as a Magistrate has in relation to proceedings in a Local Court.

(6) A Judge or Magistrate who has given consent under this section may, by instrument in writing, revoke the consent.

(7) The Attorney General may, by instrument in writing, amend or revoke a declaration under this section.

6 Act to bind Crown

This Act binds the Crown in right of New South Wales and, in so far as the legislative power of the Parliament of New South Wales permits, the Crown in all its other capacities.

Part 2 Regulation of installation, use and maintenance of surveillance devices

Note—

Offences in this Part must be dealt with on indictment (see section 5 of the *Criminal Procedure Act 1986*). However, those listed in Part 10 of Table 2 of Schedule 1 to that Act may be dealt with summarily.

7 Prohibition on installation, use and maintenance of listening devices

(1) A person must not knowingly install, use or cause to be used or maintain a listening device:

(a) to overhear, record, monitor or listen to a private conversation to which the person is not a party, or

(b) to record a private conversation to which the person is a party.

Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

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

(a) the installation, use or maintenance of a listening device in accordance with a

warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation,

(b) the installation, use or maintenance of a listening device in accordance with the *Telecommunications (Interception and Access) Act 1979*, or any other law, of the Commonwealth,

(c) the unintentional hearing of a private conversation by means of a listening device,

(d) the use of a listening device to record a refusal to consent to the recording of an interview by a member of the NSW Police Force in connection with the commission of an offence by a person suspected of having committed the offence,

(e) the use of a listening device and any enhancement equipment in relation to the device solely for the purposes of the location and retrieval of the device or equipment,

(f) the use of a listening device, being a device integrated into a Taser issued to a member of the NSW Police Force, to record the operation of the Taser and the circumstances surrounding its operation.

(3) Subsection (1) (b) does not apply to the use of a listening device by a party to a private conversation if:

(a) all of the principal parties to the conversation consent, expressly or impliedly, to the listening device being so used, or

(b) a principal party to the conversation consents to the listening device being so used and the recording of the conversation:

(i) is reasonably necessary for the protection of the lawful interests of that principal party, or

(ii) is not made for the purpose of communicating or publishing the conversation, or a report of the conversation, to persons who are not parties to the conversation.

(4) Subsection (1) does not apply to the use of a listening device to record, monitor or listen to a private conversation if:

(a) a law enforcement officer is a party to the private conversation, and

(b) the law enforcement officer is a participant (within the meaning of the *Law Enforcement (Controlled Operations) Act 1997*) in an authorised operation (within the meaning of that Act) who is using an assumed name or assumed identity.

8 Installation, use and maintenance of optical surveillance devices without consent

(1) A person must not knowingly install, use or maintain an optical surveillance device on

or within premises or a vehicle or on any other object, to record visually or observe the carrying on of an activity if the installation, use or maintenance of the device involves:

(a) entry onto or into the premises or vehicle without the express or implied consent of the owner or occupier of the premises or vehicle, or

(b) interference with the vehicle or other object without the express or implied consent of the person having lawful possession or lawful control of the vehicle or object.

Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

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

(a) the installation, use or maintenance of an optical surveillance device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation,

(b) the installation, use or maintenance of an optical surveillance device in accordance with a law of the Commonwealth,

(c) the use of an optical surveillance device and any enhancement equipment in relation to the device solely for the purpose of the location and retrieval of the device or equipment,

(d) the installation, use or maintenance of an optical surveillance device by a law enforcement officer in the execution of a search warrant or crime scene warrant (including the use of an optical surveillance device to record any activity in connection with the execution of the warrant),

Note—

See also section 255 of the *Children and Young Persons (Care and Protection) Act 1998*.

(e) the use of an optical surveillance device, being a device integrated into a Taser issued to a member of the NSW Police Force, to record the operation of the Taser and the circumstances surrounding its operation.

(3) In this section:

crime scene warrant has the same meaning as it has in the *Law Enforcement (Powers and Responsibilities) Act 2002*.

search warrant means a search warrant issued under:

(a) any of the following provisions of the *Law Enforcement (Powers and Responsibilities) Act 2002*:

(i) Division 2 (Police powers relating to warrants) of Part 5,

(ii) Part 6 (Search, entry and seizure powers relating to domestic violence offences),

(iii) Division 1 (Drug premises) of Part 11, or

(b) section 40 of the *Independent Commission Against Corruption Act 1988*, or

(c) section 11 of the *New South Wales Crime Commission Act 1985*, or

(d) Division 2 or 3 of Part 4 of the *Criminal Assets Recovery Act 1990*,

(e) section 45 of the *Police Integrity Commission Act 1996*.

9 Prohibition on installation, use and maintenance of tracking devices

(1) A person must not knowingly install, use or maintain a tracking device to determine the geographical location of:

(a) a person—without the express or implied consent of that person, or

(b) an object—without the express or implied consent of a person in lawful possession or having lawful control of that object.

Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

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

(a) the installation, use or maintenance of a tracking device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation,

(b) the installation, use or maintenance of a tracking device in accordance with a law of the Commonwealth,

(c) the installation, use or maintenance of a tracking device for a lawful purpose.

10 Prohibition on installation, use and maintenance of data surveillance devices

(1) A person must not knowingly install, use or maintain a data surveillance device on or in premises to record or monitor the input of information into, or the output of information from, a computer on the premises if the installation, use or maintenance of the device involves:

(a) entry onto or into the premises without the express or implied consent of the owner or occupier of the premises, or

(b) interference with the computer or a computer network on the premises without

the express or implied consent of the person having lawful possession or lawful control of the computer or computer network.

Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

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

(a) the installation, use or maintenance of a data surveillance device in accordance with a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation,

(b) the installation, use or maintenance of a data surveillance device in accordance with a law of the Commonwealth.

11 Prohibition on communication or publication of private conversations or recordings of activities

(1) A person must not publish, or communicate to any person, a private conversation or a record of the carrying on of an activity, or a report of a private conversation or carrying on of an activity, that has come to the person's knowledge as a direct or indirect result of the use of a listening device, an optical surveillance device or a tracking device in contravention of a provision of this Part.

Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

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

(a) if the communication or publication is made:

(i) to a party to the private conversation or activity, or

(ii) with the consent, express or implied, of all the principal parties to the private conversation or activity, or

(iii) for the purpose of investigating or prosecuting an offence against this section, or

(iv) in the course of proceedings for an offence against this Act or the regulations,

(b) if the communication or publication is no more than is reasonably necessary in connection with an imminent threat of:

(i) serious violence to persons or of substantial damage to property, or

(ii) commission of a serious narcotics offence.

(3) A person who obtains knowledge of a private conversation or activity in a manner that does not involve a contravention of a provision of this Part is not prevented from

communicating or publishing the knowledge so obtained even if the same knowledge was also obtained in a manner that contravened this Part.

12 Possession of record of private conversation or activity

(1) A person must not possess a record of a private conversation or the carrying on of an activity knowing that it has been obtained, directly or indirectly, by the use of a listening device, optical surveillance device or tracking device in contravention of this Part.

Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

(2) Subsection (1) does not apply where the record is in the possession of the person:

(a) in connection with proceedings for an offence against this Act or the regulations, or

(b) with the consent, express or implied, of all of the principal parties to the private conversation or persons who took part in the activity, or

(c) as a consequence of a communication or publication of that record to that person in circumstances that do not constitute a contravention of this Part.

13 Manufacture, supply and possession of listening and other devices for unlawful use

(1) A person must not:

(a) manufacture, or

(b) supply or offer to supply, or

(c) possess,

a data surveillance device, listening device, optical surveillance device or tracking device with the intention of using it, or it being used, in contravention of this Part.

Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

(2) In subsection (1), ***supply*** includes sell and distribute.

14 Communication and publication of information from the use of a data surveillance device

(1) A person must not publish, or communicate to any person, any information regarding the input of information into, or the output of information from, a computer obtained as a direct or indirect result of the use of a data surveillance device in contravention of this Part.

Maximum penalty: 500 penalty units (in the case of a corporation) or 100 penalty units or 5 years imprisonment, or both (in any other case).

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

(a) to a communication or publication made:

(i) to the person having lawful possession or control of the computer, or

(ii) with the consent, express or implied, of the person having lawful possession or lawful control of the computer, or

(iii) for the purpose of investigating or prosecuting an offence against this section, or

(iv) in the course of proceedings for an offence against this Act or the regulations,

(b) if the communication or publication is no more than is reasonably necessary in connection with an imminent threat of:

(i) serious violence to persons or substantial damage to property, or

(ii) the commission of a serious narcotics offence.

(3) A person who obtains information in a manner that does not involve a contravention of this Part is not prevented from publishing or communicating the information so obtained even if the same information was also obtained in a manner that contravened this Part.

Part 3 Warrants

Division 1 Preliminary

15 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 in respect of one or more kinds of surveillance devices and more than one surveillance device of the same kind.

16 Who may issue warrants?

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

(2) An eligible Magistrate may issue:

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

(b) a retrieval warrant in respect of a tracking device under a warrant referred to in paragraph (a) if an eligible Magistrate issued the original warrant.

Division 2 Surveillance device warrants

17 Application for a surveillance device warrant

(1) A law enforcement officer (or another person on his or her behalf) may apply for the issue of a surveillance device warrant if the law enforcement officer on reasonable grounds suspects or believes that:

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

(b) an investigation into that offence is being, will be or is likely to be conducted in this jurisdiction or in this jurisdiction and in one or more participating jurisdictions, and

(c) the use of a surveillance device is necessary for the purpose of an investigation into that offence to enable evidence to be obtained of the commission of that offence or the identity or location of the offender.

(2) The application may be made to:

(a) an eligible Judge in any case, or

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

(3) An application:

(a) must specify:

(i) the name of the applicant, and

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

(b) subject to this section, must be supported by an affidavit setting out the grounds on which the warrant is sought.

(4) If a law enforcement officer believes that:

(a) the immediate use of a surveillance device is necessary for a purpose referred to in subsection (1) (c), and

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

an application for a warrant may be made before an affidavit is prepared or sworn.

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

(a) provide as much information as the eligible Judge or eligible Magistrate considers is reasonably practicable in the circumstances, and

(b) not later than 72 hours following the making of the application, send a duly sworn affidavit to the eligible Judge or eligible Magistrate, whether or not a warrant has been issued.

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

18 Remote application

(1) If a law enforcement officer believes that it is impracticable for an application for a surveillance device warrant to be made in person or that the immediate use of a surveillance device is necessary, the application may be made under section 17 by telephone, fax, e-mail or any other means of communication.

(2) If transmission by fax is available and an affidavit has been prepared, the person applying must transmit a copy of the affidavit, whether sworn or unsworn, to the eligible Judge or eligible Magistrate who is to determine the application.

19 Determining the application

(1) An eligible Judge or eligible Magistrate may issue a surveillance device warrant if satisfied:

(a) that there are reasonable grounds for the suspicion or belief founding the application for the warrant, and

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

(c) in the case of a remote application—that it would have been impracticable for the application to have been made in person or that the application could not be made in person because the surveillance device needed to be used immediately.

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

(a) the nature and gravity of the alleged offence in respect of which the warrant is sought, and

(b) the extent to which the privacy of any person is likely to be affected, and

(c) the existence of any alternative means of obtaining the evidence or information sought to be obtained and the extent to which those means may assist or prejudice the investigation, and

(d) the extent to which the information sought to be obtained would assist the investigation, and

(e) the evidentiary value of any information sought to be obtained, and

(f) any previous warrant sought or issued under this Part or a corresponding law (if known) in connection with the same offence.

20 What must a surveillance device warrant contain?

(1) A surveillance device warrant must:

(a) state that the eligible Judge or eligible Magistrate is satisfied of the matters referred to in section 19 (1) and has had regard to the matters referred to in section 19 (2), and

(b) specify:

(i) the name of the applicant, and

(ii) the alleged offence in respect of 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 or in premises or a vehicle—the premises or vehicle on or in which the use of the surveillance device is authorised, and

(vi) if the warrant authorises the use of a surveillance device in or on an object or class of object—the object or class of object in or on which the use of the surveillance device is authorised, and

(vii) if the warrant authorises the use of a surveillance device on or about the body of a person—the name of the person, and

(viii) if the warrant authorises the use of a surveillance device in respect of the conversations, activities or geographical location of a person—the name of the person (if known), and

(ix) the period during which the warrant is in force, being a period not exceeding 90 days, and

(x) the name of the law enforcement officer primarily responsible for executing the warrant, and

(xi) any conditions subject to which premises or vehicle may be entered, or a surveillance device used, under the warrant.

(2) In the case of a warrant referred to in subsection (1) (b) (vii), if the identity of the person is unknown, the warrant must state that fact.

(3) A warrant must be signed by the eligible Judge or eligible Magistrate issuing it and include his or her name.

(4) If an eligible Judge or eligible Magistrate issues a warrant on a remote application:

(a) the eligible Judge or eligible Magistrate must inform the applicant of:

(i) the terms of the warrant, and

(ii) the date on which and the time at which the warrant was issued,

and cause those details to be entered in a register kept by the Judge or Magistrate for that purpose, and

(b) the Judge or Magistrate must provide the applicant with a copy of the warrant as soon as possible.

21 What a surveillance device warrant authorises

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

(a) the use of a surveillance device on or in specified premises or a vehicle,

(b) the use of a surveillance device in or on a specified object or class of object,

(c) the use of a surveillance device in respect of the conversations, activities or geographical location of a specified person or a person whose identity is unknown,

(d) the use of a surveillance device on or about the body of a specified person.

(2) A surveillance device warrant authorises:

(a) for a warrant of a kind referred to in subsection (1) (a):

(i) the installation, use and maintenance of a surveillance device of the kind specified in the warrant on or in the specified premises or vehicle, and

(ii) the entry, by force if necessary, onto or into the premises or vehicle, or other specified premises adjoining or providing access to the premises or the vehicle, for any of the purposes referred to in subparagraph (i) or subsection (3), and

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

(i) the installation, use and maintenance of a surveillance device of the kind specified in the warrant in or on the specified object or an object of the

specified class, and

(ii) the entry, by force if necessary, onto or into any premises or vehicle where the object, or an object of the specified class, is reasonably believed to be or is likely to be, or other premises adjoining or providing access to those premises or the vehicle, for any of the purposes referred to in subparagraph (i) or subsection (3), and

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

(i) the installation, use and maintenance of a surveillance device of the kind specified in the warrant, on or in premises or a vehicle where the person is reasonably believed to be or likely to be in the future, and

(ii) the entry, by force if necessary, onto or into the premises or vehicle referred to in subparagraph (i), or other premises adjoining or providing access to those premises or the vehicle, for any of the purposes referred to in subparagraph (i) or subsection (3), and

(d) for a warrant of a kind referred to in subsection (1) (d)—the use of the surveillance device of the kind specified in the warrant on or about the body of the person specified in the warrant.

(3) Each 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 surveillance device, and

(c) the use of an assumed identity for the purpose of the installation, use, maintenance or retrieval of the surveillance device or enhancement equipment, and

(d) the disconnection of, or otherwise making inoperative, any security system for the purpose of the installation, maintenance or retrieval of the surveillance device or enhancement equipment, and

(e) the temporary removal of an object or vehicle from premises for the purpose of the installation, maintenance or retrieval of the surveillance device or enhancement equipment and the return of the object or vehicle to the premises, and

(f) the breaking open of anything for the purpose of the installation, maintenance or retrieval of the surveillance device or enhancement equipment, and

(g) the connection of the device or enhancement equipment to an electricity supply system and the use of electricity from that system to operate the surveillance

device or enhancement equipment, and

(h) the connection of the device or equipment to a telecommunications system or network and the use of that system or network in connection with the operation of the surveillance device or enhancement equipment, and

(i) the provision of assistance or technical expertise to the law enforcement officer named in the warrant in the installation, use, maintenance or retrieval of the surveillance device or enhancement equipment under the warrant.

(4) If a surveillance device remains on or in premises or a vehicle after the expiry of the surveillance device warrant authorising its installation, use and maintenance, the warrant is taken also to authorise, for the period of 10 days after that expiry, any action to be taken in respect of the retrieval of the device that would be authorised if the surveillance device warrant were a retrieval warrant.

Note—

Section 29 specifies the action that is authorised to be taken by a retrieval warrant. If a surveillance device remains on or in premises or vehicle for more than 10 days after its expiry, a retrieval warrant must be obtained under Division 3 to authorise retrieval of the device and any enhancement equipment in relation to it.

(5) 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.

(6) A law enforcement officer may use a surveillance device under a warrant only if he or she is acting in the performance of his or her duty.

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

(8) Nothing in this section authorises the doing of anything for which a warrant would be required under the *Telecommunications (Interception and Access) Act 1979* of the Commonwealth.

22 Extension and variation of surveillance device warrant

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

(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 is to be made to:

(a) an eligible Judge, if the warrant was issued by an eligible Judge, or

(b) an eligible Magistrate, if the warrant was issued by an eligible Magistrate.

(3) Sections 17 and 18 apply, with any necessary changes, to an application under this section as if it were an application for a warrant.

(4) The eligible Judge or eligible Magistrate may grant an application, subject to any conditions he or she thinks fit, if satisfied that the matters referred to in section 19 (1) still exist, having regard to the matters in section 19 (2).

(5) An eligible Judge or eligible Magistrate who grants an application must endorse the new expiry date or the other varied term on the original warrant.

(6) An application in respect of a warrant may be made under this section more than once.

23 Revocation of surveillance device warrant

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

(a) an eligible Judge, if an eligible Judge issued the warrant, or

(b) an eligible Magistrate, if an eligible Magistrate issued the warrant.

(2) An eligible Judge or eligible Magistrate may revoke a surveillance device warrant on application by or on behalf of a law enforcement officer.

(3) The eligible Judge or eligible Magistrate who revokes a warrant on the application of a law enforcement officer is taken to have notified the chief officer of the law enforcement agency of which the law enforcement officer to whom the warrant was issued is a member when the eligible Judge or eligible Magistrate revokes the warrant.

24 Discontinuance of use of surveillance device under warrant

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

(2) If the chief officer of the law enforcement agency of which the law enforcement officer concerned is a member is satisfied that 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 relevant offence or the identity or location of the offender, the chief officer must:

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

(b) cause an application to be made for the revocation of the warrant under section

23.

(3) If the chief officer is notified that the warrant has been revoked under section 23, he or she must take the steps necessary to ensure that 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, believes that 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 relevant offence or the identity or location of the offender, he or she must inform the chief officer of the law enforcement agency immediately.

Division 3 Retrieval warrants

25 Application for a retrieval warrant

(1) A law enforcement officer (or another person on his or her behalf) may apply for the issue of a retrieval warrant in respect of a surveillance device that was lawfully installed on premises, or in or on a vehicle or other object, under a surveillance device warrant and which the law enforcement officer on reasonable grounds suspects or believes is still on those premises or in or on that vehicle or object, or on other premises or in or on another vehicle or other object.

(2) The application may be made to:

(a) an eligible Judge in any case, or

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

(3) Subject to this section, an application must be supported by an affidavit setting out the grounds on which the warrant is sought.

(4) If a law enforcement officer believes that:

(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,

an application for a warrant may be made before an affidavit is prepared or sworn.

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

(a) provide as much information as the eligible Judge or eligible Magistrate considers is reasonably practicable in the circumstances, and

(b) not later than 72 hours following the making of the application, send a duly sworn

affidavit to the eligible Judge or eligible Magistrate who determined the application, whether or not a warrant has been issued.

(6) An application for a retrieval warrant is not to be heard in open court.

26 Remote application

(1) If a law enforcement officer believes that it is impracticable for an application for a retrieval warrant to be made in person, the application may be made under section 25 by telephone, fax, e-mail or any other means of communication.

(2) If transmission by fax is available and an affidavit has been prepared, the person applying must transmit a copy of the affidavit, whether sworn or unsworn, to the eligible Judge or eligible Magistrate who is to determine the application.

27 Determining the application

(1) An eligible Judge or eligible Magistrate may issue a retrieval warrant if the Judge or Magistrate is satisfied:

(a) that there are reasonable grounds for the suspicion or belief founding the application for the warrant, and

(b) in the case of an unsworn application—that it would be impracticable for an affidavit to have been sworn before the application was made, and

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

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

(a) the extent to which the privacy of any person is likely to be affected, and

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

28 What must a retrieval warrant contain?

(1) A retrieval warrant must:

(a) state that the eligible Judge or eligible Magistrate is satisfied of the matters referred to in section 27 (1) and has had regard to the matters referred to in section 27 (2), and

(b) specify:

(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 premises or vehicle or other object from which the surveillance 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 to whom the warrant is issued, or who is primarily responsible for executing the warrant, and

(vii) the conditions subject to which premises or a vehicle may be entered under the warrant.

(2) A warrant must be signed by the eligible Judge or eligible Magistrate issuing it and include his or her name.

(3) If the eligible Judge or eligible Magistrate issues a warrant on a remote application:

(a) the Judge or Magistrate must inform the applicant of:

(i) the terms of the warrant, and

(ii) the date on which and the time at which the warrant was issued,

and cause those details to be entered in a register kept by the eligible Judge or eligible Magistrate for that purpose, and

(b) the eligible Judge or eligible Magistrate must provide the applicant with a copy of the warrant as soon as practicable.

29 What a retrieval warrant authorises

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

(a) the retrieval of the surveillance device specified in the warrant and any enhancement equipment in relation to the device, and

(b) the entry, by force if necessary, onto or into the premises or vehicle where the surveillance device is reasonably believed to be, or other premises adjoining or providing access to those premises or the vehicle, for the purpose of retrieving the device and equipment, and

(c) the use of an assumed identity for the purpose of retrieval of the device and equipment, and

(d) the disconnection of, or otherwise making inoperative, any security system for the purpose of retrieving the device or equipment, and

(e) the temporary removal of an object or vehicle from premises for the purpose of retrieving the device or equipment and the return of the object or vehicle to the

premises, and

(f) the breaking open of any thing for the purpose of the retrieval of the device and equipment, and

(g) if the device or equipment is installed on or in an object, the temporary removal of the object from any place where it is situated for the purpose of the retrieval of the device and equipment and the return of the object to that place, and

(h) the provision of assistance or technical expertise to the law enforcement officer named in the warrant in the retrieval of the device or equipment.

(2) The warrant also authorises the use of the surveillance device and any enhancement equipment in relation to the device solely for the purposes of the location and retrieval of the device or equipment.

(3) Any information obtained from the use of a surveillance device and any enhancement equipment for the purposes of the location and retrieval of the device or equipment under subsection (2) must not be used, communicated or published for any other purpose and is inadmissible as evidence in any legal proceedings.

(4) 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.

30 Revocation of retrieval warrant

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

(a) an eligible Judge, if an eligible Judge issued the warrant, or

(b) an eligible Magistrate, if an eligible Magistrate issued the warrant.

(2) An eligible Judge or eligible Magistrate may revoke a retrieval warrant on application by or on behalf of a law enforcement officer.

(3) An eligible Judge or eligible Magistrate who revokes a warrant must give notice of the revocation to the chief officer of the law enforcement agency of which the law enforcement officer to whom the warrant was issued is a member.

(4) If the eligible Judge or eligible Magistrate revokes the warrant on the application of a law enforcement officer, the Judge or Magistrate is taken to have notified the chief officer under subsection (3) when the Judge or Magistrate revokes the warrant.

(5) If the chief officer of a law enforcement agency is satisfied that the grounds for issue of a retrieval warrant to a law enforcement officer of the agency no longer exist, the chief officer must cause an application to be made for the revocation of the warrant

under this section.

(6) If the law enforcement officer to whom a retrieval warrant has been issued, or who is primarily responsible for executing a retrieval warrant, believes that the grounds for issue of the warrant no longer exist, he or she must inform the chief officer of the law enforcement agency immediately.

Division 4 Emergency authorisations

31 Emergency use of surveillance devices—threat of serious personal violence or substantial property damage

(1) A law enforcement officer may use a surveillance device without a surveillance device warrant if the law enforcement officer on reasonable grounds suspects or believes that:

(a) an imminent threat of serious violence to a person or substantial damage to property or that a serious narcotics offence will be committed 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) A law enforcement officer authorised to use a surveillance device by subsection (1) may do anything that the officer could be authorised to do by a surveillance device warrant.

(3) A law enforcement officer is not authorised by this section to use a surveillance device outside this jurisdiction.

32 Emergency authorisation—continued use of authorised surveillance device in participating jurisdiction

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

(a) use of a surveillance device in this jurisdiction is authorised by section 31 in connection with an investigation into a relevant offence, and

(b) the law enforcement officer on reasonable grounds suspects or believes that:

(i) the investigation in relation to which the surveillance device is authorised in this jurisdiction is likely to extend to a participating jurisdiction, and

(ii) the use of the surveillance device in a participating jurisdiction is immediately necessary to prevent the loss of any evidence, and

(iii) the circumstances are so serious and the matter is of such urgency that the use of the surveillance device in the participating jurisdiction is warranted, and

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

(2) An application may be made orally, in writing or by telephone, fax, e-mail or any other means of communication.

(3) A senior officer may give an emergency authorisation for the use of a surveillance device on an application under subsection (1) if satisfied that:

(a) use of the surveillance device in this jurisdiction is authorised under a law of this jurisdiction, in connection with an investigation into a relevant offence, and

(b) there are reasonable grounds for the suspicion or belief founding the application.

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

33 Application for approval after use of surveillance device without warrant or under emergency authorisation

(1) Within 2 business days after a law enforcement officer uses a surveillance device without a warrant in an emergency under section 31, the law enforcement officer (or another person on his or her behalf) must apply to an eligible Judge for approval of the exercise of powers under that section.

(2) Within 2 business days after giving an emergency authorisation under section 32, a senior officer (or another person on his or her behalf) must apply to an eligible Judge for approval of the exercise of powers under the emergency authorisation.

(3) An application must specify:

(a) the name of the applicant, and

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

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

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

(5) An application is not to be heard in open court.

34 Consideration of application

(1) Before deciding an application for approval in respect of the use of a surveillance device without a warrant in an emergency under section 31, the eligible Judge must, in particular, and being mindful of the intrusive nature of using a surveillance device, consider the following:

(a) the nature of the threat of serious violence to a person or substantial damage to property or of the commission of a serious narcotics offence,

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

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

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

(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) Before deciding an application for approval in respect of an emergency authorisation given under section 32, the eligible Judge must, in particular, and being mindful of the intrusive nature of using a surveillance device, consider the following:

(a) the nature of the risk of the loss of evidence,

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

(c) the terms of the existing authorisation for the use of the surveillance device,

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

35 Eligible Judge may approve emergency use of powers

(1) After considering an application for approval in respect of the use of a surveillance device without a warrant in an emergency under section 31, the eligible Judge may approve the application if satisfied that there are reasonable grounds to suspect or believe that:

(a) there was a threat of serious violence to a person or substantial damage to

property or of the commission of a serious narcotics offence, and

(b) using a surveillance device may have helped reduce the threat, and

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

(2) After considering an application for approval in respect of an emergency authorisation given under section 32, the eligible Judge may approve the application if satisfied that:

(a) use of the surveillance device in this jurisdiction was authorised under a law of this jurisdiction, in connection with an investigation into a relevant offence, and

(b) there were reasonable grounds to suspect or believe that:

(i) there was a risk of loss of evidence, and

(ii) using the surveillance device in a participating jurisdiction may have helped reduce the risk, and

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

(3) If the eligible Judge approves an application under this section, 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 Division 2.

(4) If the eligible Judge does not approve an application under this section, the Judge may:

(a) order that the use of the surveillance device cease, and

(b) authorise, subject to any conditions the eligible Judge thinks fit, the retrieval of the surveillance device.

(5) In any case, the eligible Judge may order that any information obtained from or relating to the exercise of powers without a warrant or under the emergency authorisation, or any record of that information, be dealt with in the way specified in the order.

36 Admissibility of evidence

If the exercise of powers without a warrant in an emergency or under an emergency authorisation is approved under section 35, evidence obtained because of the exercise of those powers is not inadmissible in any proceeding merely because the evidence was obtained before the approval.

Part 4 Recognition of corresponding warrants and authorisations

37 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 (as the case requires) issued under Part 3.

38 Corresponding emergency authorisation

(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 3.

(2) Subsection (1) does not apply at any time after a Judge orders, under a provision of a corresponding law that corresponds to section 35 (4), that the use of a surveillance device under the corresponding emergency authorisation cease.

Part 5 Compliance and monitoring

Division 1 Restrictions on use, communication and publication of information

39 What is protected information?

In this Division:

protected information means:

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

(b) any information relating to:

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

(ii) an application for approval of powers exercised in an emergency without a warrant under section 31 or under an emergency authorisation, or

(iii) an application under a corresponding law for approval of powers exercised under a corresponding emergency authorisation, or

(c) any information obtained from use of a surveillance device as referred to in section 7 (4).

40 Prohibition on use, communication or publication of protected information

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

(a) the person intentionally, knowingly or recklessly uses, communicates or publishes any information, and

(b) the person knows that, or is reckless as to whether, the information is protected information, and

(c) the person knows that, or is reckless as to whether, the use, communication or publication of the information is prohibited by this section.

Maximum penalty: Imprisonment for 2 years.

Note—

Under section 16 of the *Crimes (Sentencing Procedure) Act 1999*, a court may impose a fine on a body corporate that commits this offence or an offence under subsection (2).

(2) A person is guilty of an offence against this subsection if the person commits an offence against subsection (1) in circumstances in which the person:

(a) intends to endanger the health or safety of any person or prejudice the effective conduct of an investigation into a relevant offence, or

(b) knows that, or is reckless as to whether, the disclosure of the information:

(i) endangers or will endanger the health or safety of any person, or

(ii) prejudices or will prejudice the effective conduct of an investigation into a relevant offence.

Maximum penalty: Imprisonment for 7 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 proceedings 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 believes on reasonable grounds that the use or communication is necessary to help prevent or reduce the threat of serious violence to a person, substantial damage to property or the commission of a serious narcotics offence, or

(c) the communication to the Director-General (within the meaning of the *Australian Security Intelligence Organisation Act 1979* of the Commonwealth) of protected information that relates or appears to relate to activities prejudicial to security

(within the meaning of that Act), or

(d) the use or communication of information referred to in paragraph (c) by an officer of the Australian Security Intelligence Organisation in the performance of his or her official functions, or

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

(4) Protected information may be used, published or communicated 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 relevant offence within the meaning of a corresponding law,

(b) the making of a decision whether or not to bring a prosecution for a relevant offence within the meaning of this Act or a relevant offence within the meaning of a corresponding law,

(c) a relevant proceeding within the meaning of this Act or a relevant proceeding within the meaning of a corresponding law,

(d) an investigation of a complaint against, or the conduct of, a public officer within the meaning of this Act or a public officer within the meaning of a corresponding law and the oversight of such an investigation,

(e) the making of a decision in relation to the appointment, re-appointment, term of appointment, promotion or retirement of a person referred to in paragraph (d) or the making of any managerial decision with respect to such a person,

(f) the keeping of records and making of reports by:

(i) a law enforcement agency in accordance with the obligations imposed by Division 2, or

(ii) a law enforcement agency (within the meaning of a corresponding law) in accordance with the obligations imposed by provisions of the corresponding law that correspond to Division 2,

(g) an inspection by the Ombudsman under section 48 or an inspection under a provision of a corresponding law that corresponds to section 48,

(h) an inquiry or investigation under the *Privacy and Personal Information Protection Act 1998* or of the law of a participating jurisdiction or of the Commonwealth concerning the privacy of personal information.

(5) Without limiting subsection (4), protected information may be communicated or

published by a law enforcement officer to any person with the consent of the chief officer of the law enforcement agency of which the officer is a member.

(6) A chief officer may consent to the communication of protected information under subsection (5) only if satisfied that it is necessary or desirable in the public interest for the protected information to be communicated to the person concerned and that the public interest in communicating the information outweighs any intrusion on the privacy of the person to whom it relates or of any other person who may be affected by its communication.

(7) In deciding whether to give consent the chief officer must take into consideration the manner in which the protected information will be dealt with after it is communicated to the person concerned.

(8) Subsections (3) (c) and (d) and (4) (a), (b) and (c) do not authorise the use, communication or publication of protected information in respect of the use of a surveillance device in an emergency without a warrant or in respect of an emergency authorisation or corresponding emergency authorisation unless the use of powers without the warrant or under that authorisation has been approved under section 35 or the provisions of a corresponding law that correspond to section 35.

(9) A reference in subsection (4) to a relevant offence is a reference to any relevant offence, whether or not it is the offence in respect of which the relevant surveillance device was used or the warrant or emergency authorisation was issued or given.

41 Dealing with records obtained by use of surveillance devices

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

(a) must ensure that every 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 or without a warrant in an emergency, is kept, in accordance with guidelines established by the chief officer, in a secure place that is not accessible to people who are not entitled to deal with the record or report, and

(b) must destroy or cause to be destroyed any record or report referred to in paragraph (a) if he or she is satisfied that it is not likely to be required in connection with a purpose referred to in section 40 (4) or (5).

(2) Subsection (1) does not apply to a record or report that is received into evidence in legal proceedings or disciplinary proceedings.

42 Protection of surveillance device technologies and methods

(1) In any proceeding, a person may object to the disclosure of information on the ground that 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 is satisfied that the ground of objection is made out, he or she may order that the person who has the information not be required to disclose it in the proceeding.

(3) In determining whether or not to make an order under subsection (2), the person conducting or presiding over the proceeding must take into account whether disclosure of the information:

(a) is necessary for the fair trial of the defendant or to ensure procedural fairness in any disciplinary or civil proceeding, 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 person conducting or presiding over a proceeding is satisfied that 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 person must make any orders prohibiting or restricting publication of the information that he or she considers necessary to ensure that those details are not revealed.

(6) Subsection (5) does not apply to the extent that the person conducting or presiding over the proceeding considers that the interests of justice require otherwise.

(7) In this section:

proceeding includes:

(a) a proceeding before a court, tribunal, Royal Commission or special commission of inquiry, or

(b) a proceeding before any other body or authority having power by law to require the production of documents or the answering of questions.

43 Protected information in the custody of a 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

44 Reports to eligible Judge or eligible Magistrate and Attorney General

(1) A person to whom a surveillance device warrant is issued must, within the time specified in the warrant, furnish a report, in writing, to an eligible Judge (if the warrant was issued by an eligible Judge) or eligible Magistrate (if the warrant was issued by an eligible Magistrate) and to the Attorney General:

(a) stating whether or not a surveillance device was used pursuant to the warrant, and

(b) specifying the type of surveillance device (if any) used, and

(c) specifying the name, if known, of any person whose private conversation was recorded or listened to, or whose activity was recorded, by the use of the device, and

(d) specifying the period during which the device was used, and

(e) containing particulars of any premises or vehicle on or in which the device was installed or any place at which the device was used, and

(f) containing particulars of the general use made or to be made of any evidence or information obtained by the use of the device, and

(g) containing particulars of any previous use of a surveillance device in connection with the relevant offence in respect of which the warrant was issued.

(2) A person to whom an approval is given in respect of the use of a surveillance device in an emergency without a warrant must, within the time specified by the eligible Judge who gave the approval, furnish a report, in writing, to an eligible Judge and to the Attorney General:

(a) specifying the type of surveillance device used, and

(b) specifying the name, if known, of any person whose private conversation was recorded or listened to, or whose activity was recorded, by the use of the device, and

(c) specifying the period during which the device was used, and

(d) containing particulars of any premises or vehicle on or in which the device was installed or any place at which the device was used, and

(e) containing particulars of the general use made or to be made of any evidence or information obtained by the use of the device, and

(f) containing particulars of any previous use of a surveillance device in connection

with the relevant offence in respect of which the approval was given.

(3) If the person to whom a surveillance device warrant is issued or to whom approval has been given in respect of use of a surveillance device in an emergency without a warrant has died, is no longer a law enforcement officer, is absent or is otherwise unavailable to furnish a report under subsection (1) or (2), it may be furnished by another person on his or her behalf.

(4) If a report is given to an eligible Judge or eligible Magistrate under subsection (1) or (2), the eligible Judge or eligible Magistrate may direct that any record of evidence or information obtained by the use of the surveillance device to which the report relates be brought into the Court, and a person to whom any such direction is given must comply with the direction.

(5) A record brought into the Court under subsection (4) is to be kept in the custody of the Court and may, by order of the Court, be made available to any person.

(6) A person whose application is granted under section 25 must, within the time specified for the purpose by the eligible Judge or eligible Magistrate granting the application, furnish a report, in writing, to an eligible Judge or eligible Magistrate and to the Attorney General:

(a) stating whether or not the surveillance device concerned was retrieved during the currency of the warrant, and

(b) if the surveillance device was not so retrieved, giving the reasons why it was not retrieved.

Maximum penalty (subsections (1), (2) and (6)): 20 penalty units or imprisonment for a term of 12 months, or both.

45 Annual reports

(1) The Attorney General is to prepare a report as soon as practicable after the end of each financial year, and in any event within 3 months after the end of the financial year, that includes the following information in respect of the financial year concerned:

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

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

(c) any other information relating to the use of surveillance devices and the administration of this Act that the Attorney General considers appropriate.

(2) The information referred to in subsection (1) (a) and (b) must be presented in such a

way as to identify the number of warrants issued and emergency authorisations given in respect of each different kind of surveillance device.

(3) The Attorney General may require the chief officer of a law enforcement agency to furnish such information relating to the use of surveillance devices by law enforcement officers of the agency as is necessary to enable the Attorney General to prepare the report.

(4) The Attorney General must lay (or cause to be laid) a copy of each report under this section before both Houses of Parliament within 15 sitting days after the report is prepared.

(5) If a House of Parliament is not sitting when the Attorney General seeks to lay a report before it, the Attorney General is to present a copy of the report to the Clerk of the House of Parliament.

(6) The report:

(a) is, on presentation and for all purposes, taken to have been laid before the House, and

(b) may be printed by authority of the Clerk of the House, and

(c) if so printed, is taken to be a document published by or under the authority of the House, and

(d) is to be recorded:

(i) in the case of the Legislative Council—in the Minutes of the Proceedings of the Legislative Council, and

(ii) in the case of the Legislative Assembly—in the Votes and Proceedings of the Legislative Assembly,

on the first sitting day of the House after receipt of the copy of the report by the Clerk.

46 Keeping documents connected with warrants and emergency authorisations

The chief officer of a law enforcement agency must cause to be kept records containing such information as is determined by the Attorney General in consultation with the chief officer with respect to warrants and emergency authorisations sought and obtained by, and the use of surveillance devices and information obtained from use of surveillance devices by, the agency or law enforcement officers of the agency.

47 Register of warrants and emergency authorisations

(1) The chief officer of a law enforcement agency must cause a register of warrants and emergency authorisations to be kept.

(2) The register is to specify, for each warrant issued to a law enforcement officer of the agency:

(a) the date of issue of the warrant, and

(b) the name of the eligible Judge or eligible Magistrate who issued the warrant, and

(c) the name of the law enforcement officer named in the warrant as the person primarily responsible for executing it, and

(d) the relevant offence in relation to which the warrant is issued, and

(e) the period during which the warrant is in force, and

(f) details of any variation or extension of the warrant.

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

(a) the date the emergency authorisation was given, and

(b) the name of the senior officer who gave the emergency authorisation, and

(c) the name of the law enforcement officer to whom the emergency authorisation was given, and

(d) the relevant offence in relation to which the emergency authorisation was given, and

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

Division 3 Inspections

48 Inspection of records by Ombudsman

(1) The Ombudsman must, from time to time, inspect the records of each law enforcement agency (other than the Australian Crime Commission) to determine the extent of compliance with this Act by the agency and law enforcement officers of the agency.

Note—

Under section 55 of the *Surveillance Devices Act 2004* of the Commonwealth, the Commonwealth Ombudsman is required to inspect the records of the Australian Crime Commission to determine the extent of the Commission's compliance with this Act. Under section 61 of that Act, the Commonwealth Ombudsman is required to report the results of the inspection to the Commonwealth Minister, lay the report before the Commonwealth Parliament and send a copy of the report to the Minister administering this Act.

(2) For the purpose of an inspection under this section, the Ombudsman:

(a) after notifying the chief officer of the agency, may enter at any reasonable time

premises 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 any information that the Ombudsman considers necessary, being information that is in the member's possession, or to which the member has access, and that is relevant to the inspection.

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

49 Report on inspection

(1) The Ombudsman must make a written report to the Minister at 6-monthly intervals on the results of an inspection under section 48.

(2) The Minister must, within 15 days after the receipt of the report, lay the report (or cause it to be laid) before both Houses of Parliament.

(3) If a House of Parliament is not sitting when the Minister seeks to lay a report before it, the Minister may present a copy of the report to the Clerk of the House of Parliament.

(4) The report:

(a) is, on presentation and for all purposes, taken to have been laid before the House, and

(b) may be printed by authority of the Clerk of the House, and

(c) if so printed, is taken to be a document published by or under the authority of the House, and

(d) is to be recorded:

(i) in the case of the Legislative Council—in the Minutes of the Proceedings of the Legislative Council, or

(ii) in the case of the Legislative Assembly—in the Votes and Proceedings of the Legislative Assembly,

on the first sitting day of the House after receipt of the report by the Clerk.

Division 4 General

50 Evidentiary certificates

(1) A senior officer of a law enforcement agency, or a person assisting him or her, may issue a written certificate signed by the officer or person setting out the facts he or she considers relevant with respect to:

(a) anything done by a law enforcement officer of the agency, or by a person assisting or providing technical expertise to him or her, in connection with the execution of a warrant or in accordance with an emergency authorisation, or

(b) anything done by a law enforcement officer of the agency in connection with:

(i) the communication by a person to another person of, or

(ii) the making use of, or

(iii) the making of a record of, or

(iv) the custody of a record of,

information obtained by the use of a surveillance device under a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorisation.

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

(3) Subsection (2) does not apply to a certificate to the extent that the certificate sets out facts with respect to anything done in accordance with an emergency authorisation or corresponding emergency authorisation unless the use of powers under the authorisation concerned has been approved under section 35 (Eligible Judge may approve emergency use of powers) or under a provision of a corresponding law that corresponds to section 35.

Part 6 Miscellaneous

51 Particulars of warrants sought under Part 3 to be notified to Attorney General

(1) A person seeking a warrant under Part 3 (including a warrant under section 35 (3)) must cause to be served on the Attorney General or an officer prescribed by the regulations notice of the following particulars:

(a) the relevant offence in respect of which the warrant is sought,

(b) where practicable, the type of surveillance device intended to be used,

(c) where practicable, the name of any person whose private conversation or activity is intended to be recorded or listened to by the use of the surveillance device,

(d) where practicable, the premises or vehicle on or in which the surveillance device is intended to be installed or the place at which the surveillance device is intended to be used,

(e) whether any attempt has been made to obtain by alternative means the evidence or information sought and, if so, the result of any such attempt,

(f) any other alternative means of obtaining the evidence or information sought to be obtained,

(g) the period during which the surveillance device is intended to be used,

(h) the name of the law enforcement officer primarily responsible for executing the warrant,

(i) details of any previous warrant sought or issued under Part 3 in connection with the same relevant offence.

(2) A warrant must not be issued under Part 3 (including a warrant under section 35 (3)) unless the eligible Judge or eligible Magistrate is satisfied that:

(a) a notice in respect of the warrant has been served in accordance with this section, and

(b) the Attorney General has had an opportunity to be heard in relation to the granting of the warrant.

(3) A notice required by this section to be served on a person may be served:

(a) by delivering it personally to the person, or

(b) by sending it by facsimile transmission to a number specified by the person (in correspondence or otherwise) as a number to which facsimile transmissions to that person may be sent.

52 Requirement to inform subject of surveillance

(1) Where, under a warrant issued under Part 3, a surveillance device has been used to record or listen to the private conversation of a person or to record visually or observe an activity of a person, an eligible Judge may direct the person to whom the warrant was issued to supply to that person, within a period specified by the eligible Judge, such information regarding the warrant and the use of the device as the eligible Judge may specify.

(2) An eligible Judge must not give a direction under subsection (1) unless the eligible Judge is satisfied that, having regard to the evidence or information obtained by the

use of the surveillance device and to any other relevant matter, the use of the surveillance device was not justified and was an unnecessary interference with the privacy of the person concerned.

(3) Before giving a direction under subsection (1), the eligible Judge must give the person to whom the warrant was issued an opportunity to be heard in relation to the matter.

(4) A person to whom a direction is given under subsection (1) must comply with the direction.

Maximum penalty: 20 penalty units or imprisonment for a term of 12 months, or both.

53 Use of assumed names or code-names in warrants

(1) An eligible Judge or eligible Magistrate may grant a warrant under this Act that refers to a person by an assumed name or code-name if the eligible Judge or eligible Magistrate is satisfied that it is necessary to do so to protect the safety of the person.

(2) A person may be referred to by an assumed name or code-name in a notice under section 51 or report under Part 5 if the person who furnishes the notice or report believes on reasonable grounds that use of the assumed name is necessary to protect the safety of the person referred to.

54 Service of documents

(1) A document that is authorised or required by this Act or the regulations to be served on any person may be served by:

(a) in the case of a natural person:

(i) delivering it to the person personally, or

(ii) sending it by post to the address specified by the person for the giving or service of documents or, if no such address is specified, the residential or business address of the person last known to the person giving or serving the document, or

(iii) sending it by facsimile transmission to the facsimile number of the person, or

(b) in the case of a body corporate:

(i) leaving it with a person apparently of or above the age of 16 years at, or by sending it by post to, the head office, a registered office or a principal office of the body corporate or to an address specified by the body corporate for the giving or service of documents, or

(ii) sending it by facsimile transmission to the facsimile number of the body corporate.

(2) Nothing in this section affects the operation of any provision of any other law or of the rules of a court authorising a document to be served on a person in any other manner.

55 Time for instituting proceedings for certain offences

Proceedings for an offence against this Act (other than proceedings that are to be dealt with on indictment) must be commenced within 2 years after the date on which the offence is alleged to have been committed.

56 Consent of Attorney General to prosecutions

(1) Proceedings for an offence against this Act or the regulations must not be instituted without the written consent of the Attorney General.

(2) In proceedings referred to in subsection (1), a consent to institute the proceedings purporting to have been signed by the Attorney General is evidence of that consent without proof of the signature of the Attorney General.

57 Offences by corporations

(1) If a corporation contravenes, whether by act or omission, any provision of this Act or the regulations, each person who is a director of the corporation or who is concerned in the management of the corporation is taken to have contravened the same provision if the person knowingly authorised or permitted the contravention.

(2) A person may be proceeded against and convicted under a provision pursuant to subsection (1) whether or not the corporation has been proceeded against or has been convicted under the provision.

(3) Nothing in this section affects any liability imposed on a corporation for an offence committed by the corporation against this Act or the regulations.

58 Orders for forfeiture

(1) Where a court has convicted a person of an offence against this Act or the regulations, it may, in addition to any penalty it may impose, make either or both of the following orders:

(a) an order that any surveillance device used in the commission of the offence be forfeited to the State or destroyed,

(b) an order that any record of a private conversation or activity:

(i) to which the offence relates, or

(ii) which was obtained by the use of a surveillance device to which the offence relates,

be forfeited to the State or destroyed.

(2) Before making an order under subsection (1), the court may require notice to be given to, and may hear, such persons as the court thinks fit.

(3) Without affecting any other right of appeal, an order under subsection (1) is appellable in the same manner as if it were, or were part of, a sentence imposed in respect of the offence.

(4) Where an order is made under subsection (1) that a surveillance device or record be forfeited to the State or destroyed, any police officer may seize the surveillance device or record for the purpose of giving effect to the order.

(5) A surveillance device or record forfeited to the State may be disposed of in accordance with the directions of the Commissioner of Police.

59 Regulations

(1) The Governor may make regulations, not inconsistent with this Act, for or with respect to any matter that by this Act is required or permitted to be prescribed or that is necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) The regulations may exempt, subject to compliance with any conditions specified in the regulations, from any or all provisions of this Act, as may be so specified, persons belonging to any class of persons so specified.

(3) Despite the provisions of section 39 of the *Interpretation Act 1987*, any regulation made for the purposes of subsection (2) takes effect on and from the date of expiry of the period during which either House of Parliament may, under section 41 of the *Interpretation Act 1987* disallow the regulation, whichever date is the later, or on and from a later date specified in the regulation.

(4) Except as provided by subsection (3), section 39 of the *Interpretation Act 1987* applies to any regulation.

(5) A regulation may create an offence punishable by a penalty not exceeding 40 penalty units in the case of a corporation or 20 penalty units in any other case.

60 Savings, transitional and other provisions

Schedule 1 has effect.

61 Amendment of other Acts and regulations

The Acts and regulations specified in Schedule 2 are amended as set out in that Schedule.

62 Repeal of Listening Devices Act 1984

The *Listening Devices Act 1984* is repealed.

63 Review of Act

(1) The Minister is to review this Act to determine whether the policy objectives of the Act remain valid and whether the terms of the Act remain appropriate for securing those objectives.

(2) The review is to be undertaken as soon as possible after the period of 5 years from the date of assent to this Act.

(3) A report on the outcome of the review is to be tabled in each House of Parliament within 12 months after the end of the period of 5 years.

Schedule 1 Savings, transitional and other provisions

(Section 60)

Part 1 General

1 Regulations

(1) The regulations may contain provisions of a savings or transitional nature consequent on the enactment of the following Acts:

this Act

(2) Any such provision may, if the regulations so provide, take effect from the date of assent to the Act concerned or a later date.

(3) To the extent to which any such provision takes effect from a date that is earlier than the date of its publication in the Gazette, the provision does not operate so as:

(a) to affect, in a manner prejudicial to any person (other than the State or an authority of the State), the rights of that person existing before the date of its publication, or

(b) to impose liabilities on any person (other than the State or an authority of the State) in respect of anything done or omitted to be done before the date of its publication.

Part 2 Provisions consequent on enactment of this Act

2 Definition

In this Part:

repealed Act means the *Listening Devices Act 1984*.

3 Warrants authorising use of listening devices under repealed Act

(1) A warrant in force under Part 4 of the repealed Act immediately before the repeal of

section 16 of that Act continues in force on and after that repeal in accordance with its terms as if it were a surveillance device warrant issued under this Act.

(2) Section 16A (Retrieval of listening device after expiry of warrant) of the repealed Act applies to and in respect of a warrant referred to in subclause (1) as if it had not been repealed.

4 Pending applications for warrants authorising use of listening devices under repealed Act

(1) An application for a warrant under Part 4 of the repealed Act made, but not determined, immediately before the repeal of section 16 of that Act is to continue to be dealt with under the repealed Act as if that Act had not been repealed.

(2) A warrant issued under subclause (1) has effect in accordance with its terms as if it were a surveillance device warrant issued under this Act.

(3) Section 16A (Retrieval of listening device after expiry of warrant) of the repealed Act applies to and in respect of a warrant referred to in subclause (1) as if it had not been repealed.

5 Warrants and authorities under this Act

A warrant may be issued, or emergency authorisation given, under this Act in relation to a relevant offence that is alleged to have been committed before the commencement of this clause.

6 Use of records

Part 5 of this Act does not apply to information obtained, or a record made, by the use before the commencement of this clause of a listening device under a warrant or authority issued under the repealed Act.

Schedule 2 Amendment of Acts and regulations

(Section 61)

2.1 Commercial Agents and Private Inquiry Agents Act 2004 No 70

Section 4 Definitions

Omit "*Listening Devices Act 1984*" from section 4 (1).

Insert instead "*Surveillance Devices Act 2007*".

2.2 Criminal Procedure Act 1986 No 209

[1] Section 268 Maximum penalties for Table 2 offences

Insert after section 268 (2) (k):

(l) for an offence under Part 2 or 5 (other than section 40 (2)) of the *Surveillance Devices Act 2007*—in the case of an individual, imprisonment for 2 years, or a fine of 100 penalty units (or both), or in the case of a corporation, 200 penalty units.

[2] Schedule 1 Indictable offences triable summarily

Insert after Part 9 of Table 2:

Part 10 Offences relating to surveillance devices

19 Surveillance Devices Act 2007

An offence under Part 2 or 5 (other than section 40 (2)) of the *Surveillance Devices Act 2007*.

2.3 Electricity (Consumer Safety) Regulation 2006

Clause 35A

Insert after clause 35:

35A Exclusion from application of Part

This Part does not apply to or in respect of electrical installation work if it is carried out by a law enforcement officer (within the meaning of the *Surveillance Devices Act 2007* that is authorised by a surveillance device warrant as referred to in section 21 (3) (g) of that Act.

2.4 Independent Commission Against Corruption Act 1988 No 35

Section 19 Incidental powers

Omit "*Listening Devices Act 1984*".

Insert instead "*Surveillance Devices Act 2007*".

2.5 Law Enforcement (Powers and Responsibilities) Act 2002 No 103

[1] Section 108F Operation of Surveillance Devices Act 2007

Omit "*Listening Devices Act 1984*".

Insert instead "*Surveillance Devices Act 2007*".

[2] Schedule 1 Acts not affected by this Act

Omit "*Listening Devices Act 1984* No 69".

[3] Schedule 1

Insert in alphabetical order:

Surveillance Devices Act 2007

2.6 Police Integrity Commission Act 1996 No 28

Section 50 Surveillance devices

Omit "*Listening Devices Act 1984*".

Insert instead "*Surveillance Devices Act 2007*".

2.7 Royal Commission (Police Service) Act 1994 No 60

Section 25 Surveillance devices

Omit "*Listening Devices Act 1984*".

Insert instead "*Surveillance Devices Act 2007*".

2.8 State Records Regulation 2005

Schedule 2 Provisions excepted from operation of section 21

Omit "*Listening Devices Act 1984*, sections 22 (Destruction of irrelevant records made by the use of a listening device) and 30 (Orders for forfeiture)".

Insert instead "*Surveillance Devices Act 2007*, section 41 (Dealing with records obtained by use of surveillance devices) and section 58 (Orders for forfeiture)".

2.9 Workplace Surveillance Act 2005 No 47

Section 3 Definitions

Omit the note to the definition of ***surveillance***.

Insert instead:

Note—

This Act does not apply to surveillance by means of a listening device. See section 4 (3) of the *Surveillance Devices Act 2007*. Camera surveillance that is regulated by this Act will also be regulated by the *Surveillance Devices Act 2007* if the camera is used to record a private conversation.