

Explanatory note

This explanatory note relates to this Bill as introduced into Parliament.

Overview of Bill

The objects of this Bill are as follows:

- (a) to regulate the installation, use, maintenance and retrieval of surveillance devices,
- (b) to restrict the use, publication and communication of information obtained through the use of surveillance devices or otherwise connected with surveillance device operations,
- (c) to establish procedures for law enforcement officers to obtain warrants or emergency authorisations for the installation, use, maintenance and retrieval of surveillance devices,
- (d) to create offences relating to the improper installation or use of surveillance devices,
- (e) to impose requirements for the secure storage and destruction of records, and the making of reports to judicial officers and Parliament, in connection with surveillance device operations,
- (f) to recognise warrants and emergency authorisations issued in other jurisdictions for the installation and use of surveillance devices,
- (g) to repeal the *Listening Devices Act 1984*,
- (h) to make consequential amendments to various other Acts and regulations.

The Bill implements (with modifications) national legislation that was developed by a Joint Working Group of the Standing Committee of Attorneys-General and the Australasian Police Ministers' Council on National Investigation Powers to facilitate the use of surveillance devices by law enforcement agencies in cross-border investigations (the **model law**). The model law was published in November 2003 in the Joint Working Group's Report on Cross-Border Investigative Powers for Law Enforcement.

The Bill applies not only in relation to cross-border investigations, but also in relation to local investigations. This will mean that law enforcement officers will be able to obtain one warrant that will apply locally and in other participating jurisdictions that have enacted the model law. The proposed Act will replace the *Listening Devices Act 1984* (the **LDA**), which regulates the use of listening devices, with legislation regulating the installation, use and maintenance not only of listening devices but also of three other categories of surveillance device. These are **data surveillance devices** (which are devices or programs capable of being used to record or monitor the input of information into, or the output of information from, computers), **optical surveillance devices** (which are devices capable of being used to record visually or observe activities) and **tracking devices** (which are electronic devices capable of being used to determine or monitor the geographical location of a person or an object).

Outline of provisions

Part 1 Preliminary

Clause 1 sets out the name (also called the short title) of the proposed Act.

Clause 2 provides for the commencement of the proposed Act on a day or days to be appointed by proclamation.

Clause 3 describes the application of the proposed Act. It will apply in addition to other legislation regulating surveillance devices.

Clause 4 defines certain words and expressions used in the proposed Act.

A **surveillance device** is defined as a data surveillance device, a listening device, an optical surveillance device or a tracking device and so as to include a device that is a combination of any 2 or more such devices and any other device prescribed by the regulations.

The LDA currently prohibits the use of listening devices to record private

conversations, except in circumstances set out in the Act, without the use of a warrant issued by an eligible judge (see section 5). A **listening device** is defined as “any instrument, apparatus, equipment or device capable of being used to record or listen to a private conversation simultaneously with its taking place”. The proposed Act defines a listening device so as not to incorporate the notion of a private conversation. It is essentially any device (other than a hearing device or similar device) capable of being used to overhear, record, monitor or listen to a conversation or words spoken by any person in conversation. However, the concept of private conversation is still used in offence provisions and a definition of **private conversation** is included in proposed section 4.

Under the proposed Act, a surveillance device warrant can only be obtained in relation to offences that fall within the definition of **relevant offence**. This is defined as an offence against a law of New South Wales or of the Commonwealth or another State or Territory that may be prosecuted on indictment or any other offence prescribed by the regulations.

The proposed section includes definitions of **law enforcement officer** and **law enforcement agency**. Under the LDA any person may apply for a warrant to authorise the use of a listening device. Under the proposed Act, only a law enforcement officer (or person acting on his or her behalf) may do so.

The proposed section also defines **corresponding law**, **corresponding warrant**, **corresponding emergency authorisation** and **participating jurisdiction**. These definitions are used in provisions that will enable New South Wales to recognise laws in other jurisdictions that have implemented the model law and will enable warrants executed and authorisations given under those laws to be executed and acted on as if they were issued or given under the proposed Act.

Clause 5 defines **eligible Judge** and **eligible Magistrate** for the purposes of the proposed Act. The essence of the proposed section is that an eligible Judge or eligible Magistrate is a person who is a Judge of the Supreme Court or a Magistrate, respectively, who consents to being involved in the grant of warrants.

Clause 6 provides for the proposed Act to bind the Crown.

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

Proposed Part 2 replaces the offences concerning listening devices contained in Part 2 of the LDA with new offences relating to data surveillance devices, listening devices, optical surveillance devices and tracking devices.

Clause 7 makes it an offence (with specified exceptions) for a person to knowingly install, use or cause to be used, or to maintain, a listening device to overhear, record, monitor or listen to a private conversation to which the person is not a party or to record a private conversation to which the person is a party. The offence is similar to that currently contained in section 5 of the LDA although the offence under that section relates only to use of the device. It will not be an offence if the installation, use or maintenance of the listening device is authorised by a warrant, corresponding warrant, emergency authorisation or corresponding emergency authorisation or if the surveillance is done in accordance with a law of the Commonwealth. It will also not be an offence if a listening device is used by law enforcement officers for participant monitoring in the course of a controlled operation.

Clause 8 creates a new offence of installing, using or maintaining an optical surveillance device to record visually or observe the carrying on of an activity if the installation, use or maintenance of the device involves entry onto or into premises or a vehicle without the consent of the owner or occupier of the premises or vehicle or interference with a vehicle or other object without the consent of the person having lawful possession or lawful control of the vehicle or object. It will not be an offence if the installation, use or maintenance of the optical surveillance device is authorised by a warrant, corresponding warrant, emergency authorisation or corresponding

emergency authorisation or if the surveillance is done in accordance with a law of the Commonwealth and in other specified circumstances.

Clause 9 creates a new offence of knowingly installing, using or maintaining a tracking device to determine the geographical location of a person or an object without the consent of the person or the person having lawful possession or control of the object. It will not be an offence if the installation, use or maintenance of the tracking device is authorised by a warrant, corresponding warrant, emergency authorisation or corresponding emergency authorisation or if the surveillance is done in accordance with a law of the Commonwealth or for a lawful purpose.

Clause 10 creates a new offence of a person knowingly installing, using or maintaining a data surveillance device to record or monitor the input of information into, or the output of information from, a computer if the installation, use or maintenance of the device involves entry onto or into premises without the consent of the owner or occupier of the premises or interference with a computer or computer network on premises without the consent of the person having lawful possession or lawful control of the computer or computer network. It will not be an offence if the installation, use or maintenance of the data surveillance device is authorised by a warrant, corresponding warrant, emergency authorisation or corresponding emergency authorisation or if the surveillance is done in accordance with a law of the Commonwealth.

Clause 11 makes it an offence (with specified exceptions) to publish or communicate to any person a private conversation or 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 result of the use of a surveillance device in contravention of proposed Part 2. To the extent the proposed section deals with private conversations it is similar to section 6 of the LDA.

Clause 12 makes it an offence to possess a record of a private conversation or the carrying on of an activity knowing that it has been obtained in contravention of proposed Part 2. It replaces and essentially restates, with modifications to cover surveillance devices generally, section 8 of the LDA.

Clause 13 makes it an offence to manufacture, supply or offer to supply, or possess a surveillance device with the intention of it being used in contravention of proposed Part 2. It replaces and essentially restates, with modifications to cover surveillance devices generally, section 9 of the LDA.

Clause 14 creates a new offence that prohibits (with specified exceptions) a person from publishing or communicating any information regarding the input of information into, or the output of information from, a computer obtained as a result of the use of a data surveillance device in contravention of proposed Part 2.

Part 3 Warrants

Division 1 Preliminary

Clause 15 sets out the types of warrants that may be obtained. These are surveillance device warrants and retrieval warrants. A surveillance device warrant may be issued in respect of a data surveillance device, a listening device, an optical surveillance device or a tracking device. It may be issued in respect of one or more kinds of device and more than one device of the same kind. Under proposed section 17 the application for the warrant must specify the kind or kinds of surveillance devices sought to be obtained.

A retrieval warrant authorises the retrieval of a surveillance device when the warrant under which the device was installed has expired and a period of 10 days has passed or when the warrant is no longer applicable. For example, the device may be located in different premises from those initially authorised under the surveillance device warrant. This differs from section 16A of the LDA. Under that section it is not necessary to obtain a new warrant if a listening device remains on premises after the expiry of the warrant authorising its installation as that warrant is taken to continue

in force for a period of 10 days after its expiry (or such longer period as is allowed by a Supreme Court judge). Section 16A requires and authorises the listening device to be retrieved in that extended period.

Clause 16 provides for an eligible Judge to deal with an application for any warrant and confers power on an eligible Magistrate to issue warrants with respect to tracking devices only. The LDA similarly provides for the issue of warrants by Supreme Court judges and enables other regulations to be made conferring this power on other eligible judicial officers.

Division 2 Surveillance device warrants

Clause 17 provides for a law enforcement officer (or another person on his or her behalf) to apply for the issue of a surveillance device warrant. The law enforcement officer must have reasonable grounds to suspect or believe that a relevant offence has been, is being, is about to be or is likely to be committed, that 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 that 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. Aside from the expansion to cover surveillance devices generally and use of them in participating jurisdictions, the proposed section is similar to section 16 of the LDA.

The application must specify the applicant's name and the nature and duration of the warrant sought (including the kind or kinds of surveillance devices to be authorised) and be supported by an affidavit. Warrant applications are not to be heard in open court.

Clause 18 enables the making of warrant applications by telephone, fax, e-mail or other means of communication where it is impracticable for a law enforcement officer to apply in person or where immediate use of a surveillance device is necessary. Aside from the expansion to cover surveillance devices generally and use of them in participating jurisdictions the proposed section is similar to section 18 of the LDA.

Clause 19 sets out the matters an eligible Judge or eligible Magistrate must take into account when determining warrant applications. These are very similar to matters to be taken into account under section 16 (2) of the LDA.

Clause 20 sets out the matters to be specified in a surveillance warrant. Aside from the expansion to cover surveillance devices generally the proposed section is similar to section 16 (4) of the LDA. As in the LDA the warrant must specify the period during which the warrant is to be in force. Under the proposed Act this is a period not exceeding 90 days, in contrast to the LDA which limits the period to a maximum of 21 days. Proposed section 20 also requires the name of the applicant for the warrant and the officer primarily responsible for executing the warrant to be specified.

Clause 21 sets out the things a surveillance device warrant authorises. A warrant will authorise a surveillance device to be installed, used, maintained and retrieved in relation to particular premises, an object or class of objects or a person. It authorises law enforcement officers to enter (by force if necessary) premises or other specified premises providing access to those premises to install the device or to remove an object from premises in order to install or retrieve the device. The warrant also authorises various other things such as use of an electricity supply system to operate the device and to obtain technical assistance. The warrant also authorises 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 (for example, by disabling an alarm system in order to install the device).

The authority conferred by a warrant will be subject to any conditions that are specified in the warrant.

Clause 22 enables a law enforcement officer who has been issued with a warrant to

apply to an eligible Judge or eligible Magistrate (depending on who issued the warrant) to extend or vary the warrant. There is no equivalent in the LDA (under that Act application would need to be made for the issue of a further warrant).

Clause 23 enables an eligible Judge or eligible Magistrate (depending on who issued the warrant) to revoke a surveillance device warrant at any time before it expires.

Clause 24 imposes obligations on the chief officer of a law enforcement agency to ensure that the use of a surveillance device is discontinued and an application is made for the warrant to be revoked if the use of the device is no longer necessary. The chief officer must also ensure use of the device is discontinued if the warrant is revoked under proposed section 23.

Division 3 Retrieval warrants

Clause 25 allows an application to be made for a retrieval warrant. The application process is similar to an application for a surveillance device warrant.

Clause 26 allows an application for a retrieval warrant to be made by telephone, fax, e-mail or other means of communication if it is impracticable for the law enforcement officer to apply in person.

Clause 27 sets out the matters that an eligible Judge or eligible Magistrate must take into account when determining an application for a retrieval warrant.

Clause 28 sets out the things a retrieval warrant must specify.

Clause 29 sets out the things a retrieval warrant authorises. It authorises (among other things) the retrieval of the device specified in the warrant and any enhancement equipment in relation to the device, the entry (by force if necessary) onto the premises or other specified premises providing access to those premises and the breaking open of anything to retrieve the device.

Clause 30 provides for the revocation of a retrieval warrant by an eligible Judge or eligible Magistrate (depending on who issued the warrant) before it expires.

Division 4 Emergency authorisations

Clause 31 permits a law enforcement officer of a law enforcement agency to use a surveillance device without a surveillance device warrant in limited circumstances where there is an imminent threat of serious personal violence or substantial damage to property or imminent threat of a serious narcotics offence being committed. This differs from the model law, which provides for a senior officer of a law enforcement agency to give an emergency authorisation where there is an imminent threat of serious violence to a person or of substantial damage to property.

Clause 32 enables a law enforcement officer of a law enforcement agency to apply to a senior officer of the agency for an emergency authorisation for the use of a surveillance device in a participating jurisdiction. The authorisation may be given only if the senior officer is satisfied that the use of the surveillance device in New South Wales is authorised under a law of New South Wales in connection with an investigation of a relevant offence.

Clause 33 requires a senior officer of a law enforcement agency to apply to an eligible Judge for approval of the use of a surveillance device without a warrant under proposed section 31 or 32. The application must be made within 5 days after the surveillance device is used by a law enforcement officer under proposed section 31 or authorised by the senior officer under proposed section 32.

Clause 34 sets out the things the eligible Judge must take into account when considering an application for approval under proposed section 33 with respect to emergency use of a surveillance device without a warrant under proposed section 31 or use under an emergency authorisation under proposed section 32.

Clause 35 sets out the things that an eligible Judge must be satisfied of before approving the emergency use of powers under proposed section 31 or 32. If the Judge approves the use, he or she may issue a surveillance device warrant for the continued use of the device. If the Judge does not approve the use, he or she can order that use of the device cease and authorise its retrieval. Whether the application is approved or

not, the Judge has the discretion to make orders about the information obtained from the use of the device or records of that information.

Clause 36 makes it clear that evidence obtained by emergency use of a surveillance device under proposed section 35 which is subsequently approved is not inadmissible in any proceedings simply because it was obtained before the approval. Proposed section 40 (8) prevents the use, communication or publication of information obtained by emergency use of a surveillance device if that use is not subsequently approved.

Part 4 Recognition of corresponding warrants and authorisations

Proposed Part 4 provides for the recognition of corresponding warrants and emergency authorisations. The adoption of the model law and mutual recognition of warrants across borders will mean that it will no longer be necessary to obtain a warrant in every State or Territory that a suspect enters. Once other States and Territories adopt the model law, warrants and emergency authorisations that are issued in New South Wales will be recognised as valid in those jurisdictions by virtue of provisions that mirror proposed Part 4.

Clause 37 provides that a corresponding warrant can be executed in New South Wales as if it were issued under Part 3 of the proposed Act. (A **corresponding warrant** is defined in proposed section 4 as 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.)

Clause 38 ensures that a corresponding emergency authorisation can authorise the use of a surveillance device in Victoria, for example, as if it were given under the proposed Act. If the interstate judge or court decides not to approve the emergency use of a surveillance device under a corresponding law equivalent to proposed section 35 and orders that use of the device cease, the recognition of the emergency authorisation in New South Wales will also cease.

Part 5 Compliance and monitoring

Division 1 Restrictions on use, communication and publication of information

Clause 39 defines **protected information**. It includes not only information obtained from surveillance devices under warrants and emergency authorisations, but also information that relates to the application process behind warrants and emergency authorisations or obtained as referred to in proposed section 7 (4).

Clause 40 creates two new offences. Proposed section 40 (1) prohibits a natural person or body corporate from using, communicating or publishing protected information. Proposed section 40 (2) makes it an aggravated offence to commit an offence under proposed section 40 (1) in circumstances where the protected information is used, communicated or disclosed with the intention or knowledge that it will endanger a person's health or prejudice the effective investigation of an offence or being reckless as to that result. The new offences do not apply in the circumstances set out in proposed section 40 (4) (for example, if the protected information is used, communicated or published because it is necessary to do so to investigate any relevant offence or the information is in the public domain).

Clause 41 requires the chief executive officer of a law enforcement agency to ensure that records or reports obtained by the use of surveillance devices by law enforcement officers of the agency are kept in secure places that are not accessible to people who are not entitled to deal with them and also requires the officer to destroy or cause such records to be destroyed when they are no longer required for any of the purposes set out in proposed section 40 (4) or (5).

Clause 42 enables a person to object to the disclosure of information in proceedings before a court and certain other bodies and authorities on the ground that the

information could reasonably be expected to reveal details of surveillance device technology or methods of installation, use or retrieval of surveillance devices. A person conducting or presiding over the proceedings concerned may order that the information not be disclosed after taking into account whether disclosure is necessary for a fair trial or is in the public interest.

Clause 43 makes it clear that 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

Clause 44 requires a person to whom a surveillance device warrant is issued, or whose emergency use of a device without a warrant is approved, to furnish a report to an eligible Judge or eligible Magistrate (depending on who issued the warrant or gave the approval) and the Attorney General setting out specified details about use of the surveillance device. The requirement is similar to that relating to listening devices contained in section 19 of the LDA.

Clause 45 requires the Attorney General to prepare an annual report with respect to specified information concerning applications for warrants and emergency authorisations made during a financial year. The Attorney General is required to prepare the report not later than 3 months after the end of the year and to lay or cause a copy of the report to be laid before each House of Parliament within 15 days after it is prepared. The Attorney General may require the chief executive officer of a law enforcement agency to furnish such information concerning use of surveillance devices by the agency as may be necessary for the preparation of the report. This is a more comprehensive requirement than that contained in section 23 of the LDA.

Clause 46 requires the chief officer of a law enforcement agency to cause to be kept such records as may be determined by the Attorney General in consultation with the chief officer relating to the use of surveillance devices.

Clause 47 requires the chief officer to cause a register of warrants and emergency authorisations to be kept.

Division 3 Inspections

Clause 48 requires the Ombudsman to inspect records of a law enforcement agency (other than the Australian Crime Commission) to determine the extent of compliance with the proposed Act by the agency and the law enforcement officers of the agency. There is no equivalent oversight in the LDA.

Clause 49 requires the Ombudsman to report to the Minister at 6-monthly intervals on the results of inspections under proposed section 48 and requires the Minister to lay or cause to be laid each report in each House of Parliament within 15 days after it is received.

Division 4 General

Clause 50 enables certain evidentiary certificates relating to things done in connection with the execution of warrants and emergency authorisations and the use of information obtained from use of surveillance devices under warrants and authorisations to be issued by senior law enforcement officers and their assistants.

Part 6 Miscellaneous

Clause 51 requires a person seeking the issue of a warrant to notify the Attorney General of certain particulars relating to the warrant.

Clause 52 enables an eligible Judge to direct a person to whom a surveillance device warrant is issued to supply the person the subject of surveillance by the device with specified information about its use within a time specified by the Judge.

Clause 53 authorises the use of an assumed name or code-name in issuing a warrant if the eligible Judge or eligible Magistrate is satisfied that it is necessary to do so to protect the safety of any person.

Clause 54 makes provision for the service of documents under the proposed Act.

Clause 55 states the period within which proceedings for offences against the

proposed Act must be commenced.

Clause 56 requires the consent of the Attorney General to the institution of proceedings for offences against the proposed Act or regulations.

Clause 57 describes the liability imposed on a director or person concerned in the management of a corporation if the corporation contravenes any provision of the proposed Act or regulations.

Clause 58 enables a court to order the forfeiture and destruction of surveillance devices and records in certain circumstances.

Clause 59 enables the Governor to make regulations for the purposes of the proposed Act.

Clause 60 is a formal provision that gives effect to the savings, transitional and other provisions set out in Schedule 1.

Clause 61 is a formal provision that gives effect to the amendments to the Acts and regulations set out in Schedule 2.

Clause 62 repeals the *Listening Devices Act 1984*.

Clause 63 provides for the review of the proposed Act in 5 years.

Schedule 1 Savings, transitional and other provisions

Schedule 1 contains savings, transitional and other provisions consequent on the enactment of the proposed Act.

Schedule 2 Amendment of Acts and regulations

Schedule 2 amends the Acts and regulations specified in the Schedule.

With the exception of the amendments to the *Criminal Procedure Act 1986* contained in Schedule 2.2 and to the *Electricity (Consumer Safety) Regulation 2006* in Schedule 2.3, the amendments are consequential in nature.

The amendments to the *Criminal Procedure Act 1986* in Schedule 2.2 provide for offences in Parts 2 and 5 of the proposed Act (other than that in proposed section 40 (2)), which are indictable offences, to be dealt with summarily by a Local Court unless the prosecutor elects for them to be dealt with on indictment (Schedule 2.2 [2]).

The maximum penalty that may be imposed by the Local Court will be, in the case of an individual, 2 years, or a fine of 100 penalty units (or both) or, in the case of a corporation, 200 penalty units (Schedule 2.2 [1]).

The amendment to the *Electricity (Consumer Safety) Regulation 2006* in Schedule 2.3 provides that the requirements of Part 1 (Electrical installation work) of Chapter 3 of the Regulation do 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 proposed Act that is authorised by a surveillance device warrant as referred to in proposed section 21 (3) (g) of that Act. This means that such electrical installation work need not comply with the standards and requirements for electrical installation work set out in clause 32 of that Regulation or conduct the safety and compliance tests required by clause 33.