2010

LEGISLATIVE ASSEMBLY FOR THE AUSTRALIAN CAPITAL TERRITORY

CRIMES (SURVEILLANCE DEVICES) BILL 2010

EXPLANATORY STATEMENT

Circulated by authority of
Simon Corbell MLA
Attorney General

Crimes (Surveillance Devices) Bill 2010

Outline

Background and Context:

In June 2009 the *Government Report on Serious Organised Crime Groups and Activities* (the SOC Report) noted that:

> The ACT is uniquely in the position where it can afford to respond in a timely and informed fashion by examining the legislative responses in all other Australian jurisdictions, and international trends and developments to ensure that the ACT maintains a robust position against serious organised crime groups and activities [at page 46].

The SOC Report also explained the national process to make consistent cross-border laws dealing with criminal investigation:

> In 2002, the Leaders Summit on Terrorism and Multi-jurisdictional Crime agreed to the development of model laws and mutual recognition for a national set of powers for cross border investigations covering controlled operations, assumed identities legislation, surveillance devices and witness anonymity. These powers are often used across jurisdictional borders and involve covert methods of investigation. The creation of a national set of investigative powers is intended to facilitate seamless law enforcement across jurisdictions [at page 6].

The task of developing the model laws was given to a national Joint Working Group established by the Standing Committee of Attorneys-General and the Australasian Police Ministers Council (the JWG). The JWG was chaired by the Commonwealth, and included representatives from law enforcement agencies and justice departments in each jurisdiction.

In February 2003, the JWG published a Discussion Paper titled *Cross-Border Investigative Powers for Law Enforcement*. The Discussion Paper was designed to facilitate public consultation on the model legislation by providing an overview of the existing law in each jurisdiction, and setting out the proposed provisions with an accompanying commentary. The JWG received 19 written submissions in response to the Discussion Paper.

Following this, the JWG released the *Cross-Border Investigative Powers for Law Enforcement – Report November 2003* which included a model Bill drafted to address issues raised during the consultation process (‘*JWG Report’*). This model bill covered controlled operations, assumed identities, surveillance devices and the protection of witness identifies.

This explanatory statement draws upon the commentary to the model Bill as set out in the JWG Report.

Purpose of the Bill

The *Crimes (Surveillance Devices) Bill 2010* will provide the ACT with a legal framework for a surveillance devices warrants scheme. The scheme will authorise the use of surveillance devices by law enforcement officer in the ACT that can also be used in other jurisdictions with corresponding law. Conversely, the Bill will enable other jurisdictions with corresponding law to use their surveillance devices warrants in the ACT.

The warrant scheme contained in this Bill will cover four categories of surveillance devices:

- Data surveillance devices: those devices, equipment or programs that are capable of being used to record or monitor data entered into or received by a computer on an ongoing basis;
- Listening devices: those devices monitor and record conversations and other audio emissions in the open air;
- Optical surveillance devices: those devices include cameras, video recorders and other devices that permit an image to be seen and/or recorded; and
- Tracking devices: those devices emit a radio signal that allows the movement of a vehicle or object to which they are attached to be monitored.

The use of surveillance technology has proven to be an effective tool to detect and prevent serious organised crime. In the Final Report of the Wood Royal Commission[1] it was considered that the use of electronic surveillance was the single most important factor in achieving a breakthrough in its investigations. The use of electronic surveillance had a number of advantages including:

- Obtaining evidence that provided a compelling, incontrovertible and contemporaneous record of criminal activity;
- The removal of the incentive to engage in process corruption;
- The opportunity to effect an arrest while a crime is in the planning state, thereby lessening the risks to lives and property; and
- Overall efficiencies in the investigation of corruption offences and other forms of criminality that are covert, sophisticated and difficult to detect by conventional methods, particularly were those involved are aware of policing methods, are conscious of visual surveillance and employ counter surveillance techniques.

To protect police and other operatives, the Bill also creates offences for communicating or publishing protected information. The dictionary defines protected information as all information relating to, or obtained from, the use of a surveillance device under warrant, emergency authorisation, and applications for, issue of, existence of or expiry of all of the above things, applications for approval of powers exercised under emergency authorisation and all corresponding matters.

[1] New South Wales, Royal Commission into the New South Wales Police Service, Final Report (1997).

Compliance with the law and monitoring of the use of surveillance devices is also built into the Bill. As the JWG Report states on page 457, it is "appropriate for there to be strict regulation on who may have access to information obtained from surveillance devices and for what purposes such information may be used". The Bill places an obligation upon the chief officer of a law enforcement agency to ensure the safe storage and destruction of records and reports that have been obtained through the use of surveillance devices.

The Bill also requires the chief officer of a law enforcement agency to provide a yearly report to the Minister on all applications for variations of surveillance device warrants, as well as the number of arrests and prosecutions commenced as a result of information obtained through the use of surveillance devices. A copy of that report will also be tabled in the Assembly.

The Australian Crime Commission (ACC) is contemplated by this Bill, as the ACC investigates organised crime on a national basis and it is intended that the ACC would be able to be involved in relevant cross-border operations. The ACC will operate under a combination of existing Commonwealth legislation together with relevant State and Territory legislation that confers powers, duties and functions on the ACC in accordance with the requirements of section 55A of the *Australian Crime Commission Act 2002* (Cth).

Like the *Crimes (Controlled Operations) Act 2008* and the *Crimes (Assumed Identities) Act 2009* this Bill will not modify the law on entrapment or improper police inducement.

Human Rights Considerations

As the JWG Report noted on page 345, the use of electronic surveillance is a "crucial tool for effective and efficient law enforcement". However, the Government acknowledges that legislation that authorises law enforcement officers to listen to the private conversations of citizens engages the right to privacy. The Bill engages the right to privacy because the Bill would authorise the covert placement of surveillance devices in a private setting, such as a person's home and the recording of information transmitted by the device.

The right to privacy contained in section 12 of the *Human Rights Act 2004* (HR Act) is based upon Article 17 of the International Covenant on Civil and Political Rights. Section 12 states that "Everyone has the right not to have his or her privacy . . . interfered with unlawfully or arbitrarily".

However, the right to privacy is not an absolute right. Section 28 of the HR Act states that "human rights may be subject only to reasonable limits set by Territory laws that can be demonstrably justified in a free and democratic society".

Indeed, there are many instances where the needs of a democratic society may affect the right to privacy. Protecting society against crime is such an example.

The European Court of Human Rights (ECHR) has determined that covert surveillance by law enforcement agencies for criminal investigation is an acceptable interference with the right to privacy provided that legal safeguards are in place.

In the 1984 case of *Malone v United Kingdom*,[2] the ECHR reviewed the controls over telephone interception in the United Kingdom and its compatibility with Article 8 of the *European Convention on Human Rights* – the right to privacy. The facts of this case related to a telephone tap being used by the police to gather information in relation to a prosecution, and Mr Malone petitioned the ECHR alleging that this was a breach of Article 8.

The Court found that a breach had occurred because the covert surveillance used to investigate a crime was not clearly incorporated into the legal rules of the state.[3] The Court also said that the existence of laws granting powers of interception of communications to aid the police in their function of investigating and detecting crime may be necessary in a democratic society for the prevention of crime in the context of the right to privacy.

The ECHR accepted that covert surveillance is an important tool for criminal investigation. The Court also noted that the exercise of such powers, because of its inherent secrecy, carries with it a danger of abuse that could have harmful consequences for democratic society. Consequently, any interference with privacy should only be regarded as necessary in a democratic society if the particular system of secret surveillance adopted contains adequate guarantees against abuse.[4]

Academic Simon Bronitt, in discussing the case of *Malone v United Kingdom* in an article discussing the use of electronic surveillance devices and human rights implications stated that:

> The European Court in reviewing the legality of the interception in Malone noted that any interference with the right to privacy protected by Art 8 must be "in accordance with the law". [*Malone v United Kingdom* (1984) 4 EHRR 330, paragraph 5 at 348] The phrase, which appears in Art 8(2) of the ECHR, is not merely a procedural requirement that State must be able to justify its action under national law, either statute or common law. Rather, the phrase relates fundamentally to the quality of the law, requiring the interference with privacy to be compatible with the rule of law in its wider sense. [*Klass v Federal Republic of Germany* **(**1978) 2 EHRR 214, paragraph 55 at 235.] As a minimum, the criteria governing interception must be publicly available, preferably embodied in law, and provide safeguards against arbitrary action. The legal rules and administrative practice governing telephone interception in this case were not sufficiently precise to comply with these requirements. [*Malone v United Kingdom, ibid,* paragraphs 67-70][5]

In the matter of *Khan v United Kingdom*[6], the ECHR examined the quality of the law

---

[2] (1985) 7 EHRR 14.
[3] (1985) 7 EHRR 14 at paragraph 79.
[4] (1985) 7 EHRR 14 at paragraph 81.
5 Bronitt, Simon; "Electronic Surveillance, Human Rights and Criminal Justice"; *Australian Journal of Human Rights*; [1997] AJHR 8; page 191.
[6] App. No. 35394/97. Judgment 12 May 2000

and not just the basic authorisation, stating that:

> [T]he phrase "in accordance with the law" not only requires compliance with domestic law but relates to the quality of that law... the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which the conditions on which public authorities are entitled to resort to such covert measures.[7]

In the 1998 case of *Valenzuela Contreras v Spain*[8] the ECHR summarised the kind of safeguards the Court would expect to see in a law of this nature to ensure compliance with human rights standards. This case related to the monitoring of a telephone line in connection with criminal proceedings against a subscriber.

At a minimum the Court expected that the law would empower a judicial officer to make an order. The law would identify who would be liable to surveillance and the nature of the offences which may give rise to an order should be stipulated. The Court also expected that there should be a limit on the duration of an order.

The scheme contemplated by the Bill more than adequately meets the safeguards. To ensure that reasonable limits apply and privacy considerations are taken into account there are a number of important safeguards and accountability measures incorporated into the Bill to ensure that surveillance powers are restrained and not abused.

The Bill empowers judicial officers to issue relevant warrants. The warrants in question are limited to known or unknown people stipulated in the warrant and must identify the specific residences or objects (for example a car or boat) subject to the installation of a surveillance device.

The Bill is limited to criminal offences. The Bill defines a 'relevant offence' as an offence against an ACT law that is punishable by imprisonment of 3 years or more, or an offence against an ACT law that is prescribed under regulation.

The Bill limits the duration of a warrant to 90 days. Any extension of a warrant is limited to a maximum of 90 days. An extension of a warrant effectively requires the law enforcement officer to make a full application, to justify the extension. Likewise, the judicial officer must consider the extension as if it was an application for a new warrant.

Further protections and safeguards built into the Bill include:

- A scheme that requires the approval by judicial officers of the covert use of surveillance devices by law enforcement officers;
- Requiring judicial officers to explicitly consider the extent to which the privacy of any person is likely to be affected and if there are suitable alternative means to obtain the evidence or intelligence when deciding whether to issue a warrant;
- The prescription of procedures to seek emergency authorisations which still require law enforcement officers to apply to a Supreme Court judge for approval of the use of the emergency powers;

[7] *Khan v United Kingdom* App. No. 35394/97. Judgment 12 May 2000; at paragraph 26.
[8] (1999) 28 EHRR 483.

- Restrictions on the use, communication and publication of information obtained from surveillance devices, including safe storage;
- Placing obligations on law enforcement agencies to record details relating to the execution of warrants and are to provide annual reports to the Attorney General on the use and effectiveness of surveillance devices;
- Requiring the Attorney General to provide the Legislative Assembly with a copy of this report every financial year; and
- The Ombudsman is granted independent oversight of the scheme and has full access to relevant records.

Crimes (Surveillance Devices) Bill 2010

Detail

Part 1 — Preliminary

Clause 1 — Name of Act

This is a technical clause that names the short title of the Act. The name of the Act would be the *Crimes (Surveillance Devices) Act 2010.*

Clause 2— Commencement

This clause enables the Act to commence by way of a notice by the Minister after the Act is notified on the Legislation Register. If the Act is not commenced within six months of notification, the provisions of the *Legislation Act 2001* will automatically commence the Act.

Clause 3— Dictionary

This is a technical clause identifying the dictionary and includes a note explaining conventions used to define words and terms.

Clause 4 — Notes

This is a technical clause explaining the status of notes to the Act.

Clause 5 — Offences against Act — application of Criminal Code etc

This clause makes it clear that the *Criminal Code 2002* applies to the Act. The subsequent Act should also be read in conjunction with the *Legislation Act 2001,* which provides for interpretation, common definitions, and legislative machinery for the ACT.

Clause 6 — Purpose of Act

Clause 6 sets out the purpose of the Act, consistent with the explanation in the 'Outline' above. The scheme will apply to both local and cross border criminal investigations.

Clause 7 — Relationship to other laws

Clause 7 specifies that the Act does not affect any other territory law that prohibits or regulates the use of surveillance devices in the ACT. The Act does not stop a law enforcement officer from using optical surveillance devices (such as spectacles, video cameras, telescopes, night vision goggles or binoculars) in a place where the presence of a police officer is not an offence. Law enforcement agencies conducting these types of investigations who wish to use a surveillance device will need to determine whether or not they need to obtain a warrant in light of the legislation in the jurisdiction and the operation of the common law. If the use of the surveillance device is not unlawful, then it will not be necessary to obtain a warrant. If the use of the surveillance device would be unlawful, either because it is prohibited by legislation or would otherwise contravene the common law (for example, installing the surveillance device may constitute a trespass to land or goods) then it will be necessary to obtain a

warrant. The Act is intended to apply the scheme to covert surveillance using defined types of surveillance devices.

Clause *7*(4) gives effect to the policy discussed in the *JWG Report* that the Bill does not seek to limit a court's discretion to admit or exclude evidence in proceedings or to stay criminal proceedings in the interests of justice.

Clause 7(4) does not prevent the court from excluding evidence which was obtained as a result of criminal conduct if another reason recognised by law exists which would also justify the exclusion of the evidence. For example, if in addition to being the result of criminal activity, it would otherwise be unfairly prejudicial or otherwise unfair to the defendant to admit the evidence, it would continue to be open to the court to exclude that evidence under sections 135, 137 or 138 of the *Evidence Act 1995* (Cwlth).

Clause 7(4) would not prevent evidence obtained as a result of criminal activity from being excluded if it would otherwise be open to the court to exclude it under Part 3.4 of the *Evidence Act 1995* (Cwlth) on the basis that the evidence constitutes an improperly obtained or unreliable admission.

Clause 7(4) also does not prevent the court from excluding evidence or staying proceedings in cases that involve entrapment or inducement. In any prosecution where it is alleged that evidence is the result of inducement or entrapment, it remains open to the court to exercise its discretion to exclude evidence or stay proceedings in light of the right to a fair trial under section 21 of the *Human Rights Act 2004.*

In the ACT, it would be open to the Court to consider national and international jurisprudence discussing the considerations of whether evidence is the result of inducement or entrapment. Relevant cases include *Ridgeway v The Queen* (1995) 184 CLR 19, *Loosely v The Queen* [2001] UKHL 53, and *R v Mack* [1988] 2 SCR 903.

Clause 7(5) specifies that the *Territory Records Act 2002* and the *Freedom of Information Act 1989* do not apply to the Bill. The Government is of the view that the public interest in protecting the identity of people authorised under the Bill and protecting the criminal intelligence involved in the scheme for use of surveillance devices outweighs the public interest in disclosing information under the Acts listed.

Clause 8 — Investigation taken to be conducted in ACT

Clause 8 is intended to cover the situation where an ACT law enforcement officer is conducting or participating in an investigation wholly in another jurisdiction for the purposes of an offence against a Territory law.

For example, an investigation into a conspiracy to import drugs into the ACT from NSW where all the evidence of the offence is in NSW.

Part 2 — Warrants

Division 2.1 Introduction

Clause 9 — Kinds of warrants

Clause 9 provides for two types of warrants that may be issued under the scheme – a surveillance device warrant and a retrieval warrant.

A warrant may be issued in relation to 1 or more kinds of surveillance devices. One generic surveillance device warrant is available, rather than a different warrant for each type of devices because it makes the warrant regime less complicated. One warrant can be sought to authorise a number of devices or composite devices, rather than requiring a separate warrant for each device, or a warrant for each type of surveillance device.

Clause 10 – Who may issue warrants

Clause 10 provides that applications for warrants are made to a Supreme Court judge for any type of surveillance device warrant and to a Magistrate for a warrant for the use of a tracking device or a retrieval warrant for a tracking device.

Tracking devices are treated differently because they involve less intrusion upon privacy than other forms of surveillance devices.

The choice of either judge or magistrate provides law enforcement agencies with greater access to judicial officers in the case of obtaining tracking devices warrants which may assist in circumstances where a warrant is needed urgently at short notice.

Division 2.2 – Surveillance device warrants

Clause 11 – Application for surveillance device warrant

Clause 11 provides that a law enforcement officer (or another person on the officer's behalf) may apply for the issue of a surveillance device warrant.

The Dictionary defines 'law enforcement officer' as a police officer or a member of staff of the Australian Crime Commission, and includes a person who is seconded to a law enforcement agency, including (but not limited to) a member of a police force or police service and a police officer (however described), of another jurisdiction.

This definition is intended to include non-police employees of law enforcement agencies and reflects that civilian employees or non-police operatives are often used in order to investigate high level corruption among police officers.

Where an application is made on behalf of a law enforcement officer, the warrant will still be issued to the law enforcement officer on whose behalf the application was made.

It is the view of the government that no further restriction to the class of person who may apply by narrowing the definition is warranted as the application is to be made to

a judicial officer, and the judicial officer may only issue a warrant if satisfied in relation to each of the criteria in clause 11(1).

Clause 11(1) sets out the criteria which must exist for a law enforcement officer to make an application for a surveillance device warrant. Firstly, the officer must suspect on reasonable grounds that a relevant offence has been, is being, is about to be, or is likely to be, committed.

A relevant offence is defined in the Dictionary as any offence against an ACT law punishable by imprisonment of 3 years or more; or an offence against an ACT law that is prescribed by regulation.

The second criteria is that the law enforcement officer must suspect on reasonable grounds that an investigation into that office is being, will be or is likely to be wholly conducted in the ACT, conducted in the ACT and in 1 or more participating jurisdictions, or conducted in 1 or more participating jurisdictions.

The final criteria is that the law enforcement officer must suspect on reasonable grounds that the use of a surveillance devices in the ACT, in the ACT and in 1 or more participating jurisdiction or in 1 or more participating jurisdictions is or will be necessary in the course of that investigation for the purpose of enabling evidence or information to be obtained of the commission of the relevant offence or the identity or location of the offender.

Clause 11(2) – (6) sets out how an application, and to whom an application can be made.

Applications may be made to the court in person, or in certain circumstances, by telephone or other electronic means like facsimile or email.

Under normal procedure, applications for warrants must be made in writing and must be supported by a sworn affidavit that sets out the grounds on which the warrant is sought. The application must contain the name of the applicant, the nature and duration of the warrant sought, including the kind of surveillance devices sought to be authorised.

In circumstances where a law enforcement officer believes that the immediate use of a surveillance device is necessary and it is impracticable to prepare and swear a supporting affidavit the application is permitted to apply to the court without an affidavit. In these circumstances, the applicant must provide as much information as the court considers is reasonably practicable and, no later than 72 hours after the application is made, file a sworn affidavit with the court.

To reflect the sensitive nature of surveillance device usage and the police operational matters that may be revealed during the hearing of an application for a surveillance device warrant or retrieval warrant the application procedure is not to be heard in open court.

Clause 12 – Remote Application
If a law enforcement officer believes that it is impracticable for an application for a surveillance warrant to be made in person, the application may be made by telephone, fax, email or any other means of communication. Under Clause 13 the Magistrate or Judge deciding the application must also be satisfied that it was impracticable to apply in person.

Clause 12(2) provides that if a remote application is made and transmission by fax is available and an affidavit has been prepared the person applying must send a copy of the affidavit, whether sworn or unsworn to the judge or magistrate who is to decide the application.

Clause 13 – Deciding the application
Cause 13 provides that a Judge or Magistrate may issue a surveillance device warrant if they are satisfied that there are reasonable grounds for the suspicion founding the application for the warrant. If the application is unsworn, the judge or magistrate must also be satisfied that it would have been impracticable for an affidavit to have been prepared or sworn before the application was made. If the application was made under clause 12, the Judge or Magistrate must also be satisfied that it would have been impracticable for the application to have been made in person.

Clause 13(2) details the matters that the judge or magistrate must have regard to in deciding whether a surveillance device warrant should be issued.

Clause 14 – What must a surveillance device warrant contain?
Clause 14 set outs what must be contained in a surveillance device warrant.

The warrant is not required to name any law enforcement officer who may use a surveillance device under the warrant as this would be impractical from an operational perspective. The warrant should name the law enforcement officer primarily responsible for executing the warrant. The name of each person involved in the actual execution of the warrant is recorded pursuant to Clause 40.

The warrant may specify conditions imposed by the issuing judge or magistrate and cannot be fore more than 90 days.

In the event that the law enforcement officer becomes aware of a change to a material particular stated in the warrant an application for amendment of the warrant should be made under clause 16. For example, the warrant states that the alleged offence in relation to which the warrant is issued is drug trafficking. During execution of the warrant information is obtained that the alleged offender is allegedly trafficking child pornography and not drugs. An application to amend the warrant should be made as soon as the applicant becomes aware of this.

Clause 15 – What a surveillance device warrant authorises
All surveillance device warrants authorise the installation, use, maintenance and retrieval of the surveillance device. As surveillance devices can malfunction, this authorisation permits re-entry onto premises to maintain the device, such as replacing

batteries, carrying out repairs, or relocating the device so that surveillance can be recorded effectively.

All warrants also authorises the entry, by force if necessary, onto specified premises, or premises where an object or person is reasonably believed to be. This power extends onto adjoining premises or premises that provide access to the specified premises.

Where the use of the device is on specified premises or a specified object, the warrant will authorise the breaking open of any thing for the purpose of installing, maintaining or retrieving the device, as well as the temporary removal and return of a vehicle or object to install, maintain or retrieve the device.

Warrants specifying premises, objects, persons or classes of objects will also authorise the use of an electricity system in connection with the operation of the surveillance device or enhancement equipment. For example, it is not always practical to operate surveillance devices using batteries, particularly where the surveillance is protracted. Authorisation prevents any argument at a later date that the device has been used unlawfully and avoids any suggestion of theft of electricity. The power to connect the device to the telephone system and to use that system does not extend to conduct that would otherwise be regulated by the Commonwealth's *Telecommunications (Interception) Act 1979*. Further, the connection can be to any object or system that may be used to transmit information in any form and the use of that object or system in connection with the operation of the surveillance device or enhancement equipment. For example, a structured cable system, cable internet/TV and Naked DSL and an alarm system.

As surveillance devices are generally highly technical the warrant also expressly extends to any persons providing assistance or technical expertise to the law enforcement officer in installing, using, maintaining or retrieving the device. It is contemplated that other assistance can include where the person under surveillance speaks a language other than English and interpreters are needed.

Given the covert nature of the surveillance 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, this would enable police officer to disable an alarm system in order to install a surveillance device.

The warrant may authorise interference with the property of a third party that is not the subject of the investigation, but only if the court is satisfied that it is necessary to do so in order to give effect to the warrant.

Although the warrants do not authorise the installation of a device on a person, they may be issued in relation to a specified class of objects so, for example, a warrant could be issued to authorise the installation of a device on any clothing worn by a specified person (class of objects).

Clause 16 – Extension and amendment of surveillance device warrant
This clause sets out how extensions of up to 90 days and amendments to surveillance device warrants may be made. The process available under section 11 and section 12 and the considerations relevant to section 13 will still apply. There is no limit on the number of times a particular warrant can be extended or varied.

Clause 17 – Revocation of surveillance device warrant
A surveillance device may be revoked at any time before the end of the period of validity stated in it in accordance with Clause 17 on application by or on behalf of a law enforcement officer.

Subsection (4) deems notification on the chief officer when the judge or magistrate revokes the warrant.

Clause 18 – Discontinuance of use of surveillance device under warrant
Clause 18 creates an obligation on the law enforcement officer to whom the warrant is issued, or who is primarily responsible for executing the warrant, an obligation to tell the chief officer of the law enforcement agency immediately if they believe that 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.

Further obligations are then placed on the chief officer to take steps necessary to ensure that use of the surveillance devices authorised by the warrant is discontinued as soon as practicable and to ensure an application is made for the revocation of the warrant under clause 17 if the chief officer is satisfied that 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 intention of this clause is to ensure that devices are not used for purposes other than those for which the warrant was granted.

Division 2.3 Retrieval warrants

Clause 19 – Application for retrieval warrant
A law enforcement officer or another person on the officer's behalf may apply to the court for a retrieval warrant for a surveillance device.

Clause 19 sets out the process and requirements for the making of such an application. The application process for a retrieval warrant mirrors the process for a surveillance devices warrant.

A separate retrieval warrant may be necessary where the surveillance device warrant has expired before law enforcement officers were able to remove the device, or where the device was installed on an object which has been relocated to different premises from those to which the initial warrant authorised access.

As there may be circumstances when it is impossible for the police to retrieve a device, retrieval is not mandatory but clause 18 provides a safeguard to ensure that the use of the device ceases once the grounds on which a warrant was issued have ceased to exist, or where the warrant has been revoked.

Clause 20 - Remote Application
Retrieval warrants may be applied for remotely under procedures which mirror the remote application process for a surveillance device warrant under Clause 12.

Clause 21 – Deciding the application
This clause states the basis upon which a judge or magistrate may issue a retrieval warrant. It requires the judge or magistrate to have regard to the extent to which the privacy of any person is likely to be affected and the public interest in retrieving the device sought to be retrieved.

Clause 22 – What must a retrieval warrant contain?
Clause 22 sets out what details must be included in a retrieval warrant. It is intended that the information required in a retrieval warrant is consistent with what is required in a surveillance warrant under Clause 14.

Clause 23 – What a retrieval warrant authorises
A retrieval warrant authorises the retrieval of a surveillance devices specified in the warrant, entry onto the premises where the devices is reasonably believed to be (including premises adjoining or providing access to those premises), the breaking open of anything for the purpose of retrieving the device, the temporary removal and return of an object on which the device is installed, the provision of assistance and the doing of any reasonable necessary to conceal the fact that the device was retrieved.

In the case of the retrieval of a tracking device, the warrant also authorises the law enforcement agency to activate the tracking device for the purposes of locating and retrieving the device. It is not intended to extend this authority to the retrieval of other types of surveillance devices that are more intrusive. This is because activating those devices (for example, optical surveillance devices) will generate more information than simply the device's location.

Clause 24 – Revocation of retrieval warrant
A retrieval warrant can be revoked in the same way as a surveillance device warrant under Clause 17.

Part 3 — Emergency authorisations

Clause 25 — Emergency authorisation – risk of serious personal violence or substantial property damage
A law enforcement officer may apply to the chief officer of the agency for an emergency authorisation for the use of a surveillance device in limited circumstances where it is not practicable in the circumstances to apply for a surveillance device warrant, even by facsimile or telephone.

To establish the threshold for making such an application a law enforcement officer must suspect or believe on reasonable grounds, in the course of an investigation, that an imminent threat of serious violence to a person or substantial damage to property exists and the use of a surveillance device is immediately necessary for the purpose of dealing with that threat and the circumstances are so serious and the matter is of such urgency that the use of a surveillance device is warranted.

The functions of a chief officer under the Bill can only be delegated to a deputy police officer (in the case of the Australian Federal Police) and the Director National Operations; a Director; an office of the Australian Crime Commission that is prescribed for regulation (in the case of the Australian Crime Commission) in accordance with Clause 44.

The rationale for the use of the emergency procedure in these circumstances is that the risk of harm and damage is so great as to justify the use of the device without court authorisation. If an emergency authorisation is given, within 2 working days after giving an emergency authorisation the chief officer (or another person on the officer's behalf) must apply to a judge for approval of the exercise of powers under the emergency authorisation in accordance with Clause 27.

A law enforcement officer using a surveillance device under an emergency authorisation will have all the powers exercisable under a surveillance device warrant.

Clause 26 – Emergency authorisation – continued use of authorised surveillance device in participating jurisdiction
Clause 26 permits a law enforcement officer to apply for an emergency authorisation for the use of a surveillance device in a participating jurisdiction.

Clause 27 – Application for approval after use of surveillance device under emergency authorisation
If an emergency authorisation is given, within 2 working days after giving an emergency authorisation the chief officer (or another person on the officer's behalf) must apply to a judge for approval of the exercise of powers under the emergency authorisation.

It is intended that if the application is approved, the judge may also issue (where requested) a surveillance device warrant for the continued use of the device.
It is intended that the application for approval mirror the warrant application process.

Clause 28 – Consideration of application
Where the emergency procedure is utilised, before deciding whether to approve the application the just must be mindful of the intrusive nature of using a surveillance device. Clause 28 sets out what must be taken into account when deciding such an application.

Clause 29 – Judge may approve emergency use of powers
Clause 29 sets out the different thresholds under which a judge may approve an application consequent to an emergency authorisation, depending on the circumstances relating to the granting of that emergency authorisation.

It is intended that if the judge approves the emergency use of powers he or she may issue a surveillance device warrant for the continued use of the surveillance devices as if it were a warrant application under Division 2. In this way, the duration of the warrant is no more than 90 days and the judge is empowered to impose conditions or restrictions on the warrant in the usual way.

If the judge does not approve an authorisation he or she may order that the use of the surveillance device cease.

In any case (regardless of whether the judge approves or does not approve an authorisation) Clause 29(5) empowers a judge to order that any information obtained from or relating to the exercise of powers under the emergency authorisation or any record of that information be dealt with in the way specified in the order. This would empower the judge to order the destruction of the material if that were appropriate.

Clause 30 – Admissibility of evidence
Clause 30 clarifies that if the exercise of powers under an emergency authorisation is approved under clause 29, evidence obtained because of the exercise of those powers is not inadmissible in any proceeding only because the evidence was obtained before the approval.

This does not prevent the court from excluding evidence which was obtained as a result of criminal conduct if another reason recognised by law exists which would also justify the exclusion of the evidence. For example, if in addition to being the result of criminal activity, it would otherwise be unfairly prejudicial or otherwise unfair to the defendant to admit the evidence, it would continue to be open to the court to exclude that evidence under sections 135, 137 or 138 of the Evidence Act 1995 (Cwlth).

Further, it would not prevent evidence obtained as a result of criminal activity from being excluded if it would otherwise be open to the court to exclude it under Part 3.4 of the *Evidence Act 1995 (Cwlth)* on the basis that the evidence constitutes an improperly obtained or unreliable admission.

It also does not prevent the court from excluding evidence or staying proceedings in cases that involve entrapment or inducement. In any prosecution where it is alleged that evidence is the result of inducement or entrapment, it remains open to the court to exercise its discretion to exclude evidence or stay proceedings in light of the right to a fair trial under section 21 of the *Human Rights Act 2004.*

Part 4 — Recognition of corresponding warrants and authorisations

Part 4 relies upon the definitions of corresponding emergency authorisation, corresponding law and corresponding law. The dictionary of the Bill defines the terms the following way:

> ***corresponding emergency authorisation*** means an authorisation given under the provisions of a corresponding law that corresponds to part 3 (emergency authorisations).

corresponding law means a law of another jurisdiction that corresponds to this Act, and includes a law of another jurisdiction that is declared by regulation to correspond to this Act.

Corresponding warrant means a warrant issued under the provisions of a corresponding law that corresponds to this Act.

This part enables surveillance device warrants and emergency authorisations issued in a participating jurisdiction to operate in the ACT as if they were issued under ACT law. It also enables the ACT to use its surveillance device warrants and emergency authorisations in a participating jurisdiction as if they had been issued in that other jurisdiction.

A participating jurisdiction is one in which a corresponding law is in operation.

It is the Government's intention that the meaning of corresponding law, and this part, should be interpreted purposefully by examining the substance of the foreshadowed Act and corresponding law. It is not intended that mutual recognition would be defeated if corresponding law was not cast in exactly the same terms as the Territory's law.

Part 5 — Compliance and monitoring

Division 5.1 Restrictions on use, communication and publication of information
It is intended that there be strict regulation on who may have access to information obtained from surveillance devices and for what purposes such information may be used.

Clause 33 – What is protected information?
Clause 33 contains an exclusive definition of protection information. It is intended that this definition includes all information relating to, or obtained from, the use of a surveillance device under warrant, emergency authorisation, and applications for, issue of, existence of or expiry of all of the above things, applications for approval of powers exercised under emergency authorisation and all corresponding matters.

Clause 34 – Prohibition on communication or publication of protected information
Clause 34 creates a series of offences relating to the use, publication or communication of protected information.

The fault element of recklessness is applied. Under section 20(4) of the fault element of recklessness can be satisfied by proof of intention, knowledge or recklessness.

Clause 34(6) sets out the exceptions to Clause 34(1) – (5). Further Clause 34(7) sets out the purposes for which protected information may be used, communicated or published.

The Clause is not intended to hinder investigations relating to allegations of police misconduct or complaints or misconduct by public officials.

Clause 35 – Dealing with records obtained by use of surveillance devices
Clause 35 provides for the safe storage and destruction requirements for records of information and reports obtained using surveillance devices. The intention of the clause is to ensure that this information is not accessible to unauthorised persons.

Clause 36 – Protection of surveillance device technologies and methods
Clause 36 provides a process to enable an objection to be made to the disclosure of information in a proceeding 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.

In considering the objection, and whether to make orders prohibiting or restricting publication of information, the person conducting or presiding over the proceeding may take into account whether disclosure of the information is necessary for the fair trial of the defendant or is in the public interest.

It was the view of the JWG that suppression of publication would not provide adequate protection for confidential information about surveillance device technology and methodology as the information would still be disclosed to the parties to the proceedings. The JWG was of the view that greater protection was needed for this highly sensitive information. A failure to provide this information could undermine the public interest in the effective investigation of crime.

Clause 37 – Protection information in the custody of a court
Clause 37 provides 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 5.2 Reporting and record-keeping

Clause 38 - Annual reports
Clause 38 obliges the relevant chief officer to provide a report to the Minister on listed information in relation to the immediately preceding financial year.

Clause 38 (1) (a) to (g) sets out what must be included in the report to the Minister.

Clause 38 (1) (h) enable the Minister to request information considered appropriate relating to the use of surveillance devices and the administration of this Act.

Clause 38(3) requires the report be given to the Minister 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.

Clause 38(4) provides that the Minister must table the chief officer's report in the Legislative Assembly within 15 sitting days from the day that the Minister receives the report.

This is consistent with the annual reporting requirements relevant to the *Crimes (Controlled Operations) Act 2008* and the *Crimes (Assumed Identities) Act 2009*.

Clause 39 – Keeping documents connected with warrants and emergency authorisations
Clause 39 lists the documents the chief officer must keep to ensure compliance with the reporting requirements in this Bill.

Clause 40 – Other records to be kept
The model bill prepared by the JWG proposed that the law enforcement officer to whom a warrant was issued, or who executed a warrant must report back to the issuing court on the use of the surveillance device(s) under the warrant. This was to ensure that law enforcement agencies are accountable for the use of surveillance devices.

The Government rejects the need for the report to be provided to the issuing court but sees the merit in ensuring that the information that is proposed to be contained within the report is recorded and kept.

The Government is of the view that the reporting requirements to the Minister, the threshold issues considered by the court when considering applications under the Bill, the threshold issues that exist before an application can be made, the inspection powers of the Ombudsman and the availability of challenges to the admissibility of evidence in accordance with the rule law are sufficient accountability measures.

Protected information can still be used, communicated or published if necessary for "a proceeding concerning the validity of a warrant, emergency authorisation, corresponding warrant or corresponding emergency authorising." This is included in the definition of "relevant proceeding" contained within the Dictionary to the Bill.

The requirement of the Chief Officer to keep and record the exact particulars which were proposed by the JWG to be included in the Report to the judge or magistrate meet the accountability objective stated as the purpose for the inclusion of the clause in the model bill.

Clause 41 – Register of warrants and emergency authorisations
The purpose of this clause is to require law enforcement agencies to keep a register of warrants and a register of emergency authorisations to provide an overview for any inspecting body of the warrants and emergency authorisations that have been issued.

Division 5.3 — Inspections

Clause 42 — Inspection of records by ombudsman
Clause 42 establishes independent oversight of the foreshadowed Act. The clause enables the ombudsman to examine records made under the Act and empowers the ombudsman to have full access to relevant records.

The ombudsman must prepare a report on the inspection results under the terms of the *Annual Reports (Government Agencies) Act 2004.* The ombudsman's report must

comment on the adequacy of the records and the cooperation given to the ombudsman by the agency.

The report must not include any information that could possibly endanger anyone, prejudice an investigation or prosecution, or compromise any operational matter.

This provision differs from the *JWG Report* and model Bill. The provision follows the precedent set in section 31 of Crimes *(Controlled Operations) Act 2008* which mandates inspection by the ombudsman. Whilst inspection is not mandated under the Bill, a report on any inspection under the section is the preceding financial year is required.

Division 5.4 — General

Clause 43 – Evidentiary certificates

This clause is based on a similar provision contained within the Telecommunications (Interpretation) Act 1979 (Cwth). It allows the chief officer of a law enforcement agency, or a person assisting the officer, to issue an evidentiary certificate to provide evidence about the actions of law enforcement officers in connection with the execution of surveillance devices warrants or information obtained by the use of surveillance devices under a warrant. It does not prevent experts and other witnesses from being called to give evidence in person or be cross-examined where permitted.

Clause 44 — Delegation

Clause 44 provides that except as provided by the clause, and despite any other Act or law to the contrary, the function of a chief officer under the Bill must not be delegated to any other person.

Clause 44(2) and (3) permit the functions of a chief officer under the Bill to be delegated to a deputy police officer (in the case of the Australian Federal Police) and the Director National Operations; a Director; an office of the Australian Crime Commission that is prescribed for regulation (in the case of the Australian Crime Commission

Clause 45 — Regulation-making power

Clause 45 authorises the Executive to make regulations for the Act.

Dictionary

The Bill includes a dictionary which draws upon the dictionary of the *Legislation Act 2001* and provides definitions for this Bill.

To remove any doubt, the meaning of corresponding law is intended to enable laws of other jurisdictions that substantially correspond with the ACT's law to be treated as corresponding law without the necessity to list every law in regulation. The regulation making power is intended to be used to enable another law to be declared despite the fact that the law does not substantially correspond to the ACT's law. It is the intention of the Government that the assessment of correspondence would be made in deliberations between the ACT and other jurisdictions.