INFORMATION, ANALYSIS
AND ADVICE FOR THE PARLIAMENT

INFORMATION AND RESEARCH SERVICES
PARLIAMENTARY LIBRARY

Bills Digest
No. 147 2003–04

Surveillance Devices Bill 2004

ISSN 1328-8091

This paper has been prepared for general distribution to Senators and Members of the Australian Parliament. While great care is taken to ensure that the paper is accurate and balanced, the paper is written using information publicly available at the time of production. The views expressed are those of the author and should not be attributed to Information and Research Services (IRS). Advice on legislation or legal policy issues contained in this paper is provided for use in parliamentary debate and for related parliamentary purposes. This paper is not professional legal opinion. Readers are reminded that the paper is not an official parliamentary or Australian government document. IRS staff are available to discuss the paper's contents with Senators and Members and their staff but not with members of the public.

Inquiries

Members, Senators and Parliamentary staff can obtain further information from the Information and Research Services on (02) 6277 2646.

Information and Research Services publications are available on the ParlInfo database.
On the Internet the Parliamentary Library can be found at: http://www.aph.gov.au/library/

Published by Information and Research Services, Parliamentary Library,
Department of Parliamentary Services, 2004.

INFORMATION AND RESEARCH SERVICES

Bills Digest
No. 147 2003–04

Surveillance Devices Bill 2004

Jennifer Norberry
Law and Bills Digest Section
26 May 2004

Contents

Surveillance Devices Bill 2004

Date Introduced: 24 March 2004

House: House of Representatives

Portfolio: Attorney-General

Commencement: On Royal Assent

Purpose

To establish a statutory regime covering the use of surveillance devices for the investigation of Commonwealth offences and State offences with 'a federal aspect'.[1] The Bill also regulates the use of information obtained from surveillance devices and enables surveillance devices to be used in relation to child recovery orders issued under the *Family Law Act 1975*.

Background

Introduction

Among other things, the Bill is designed to:

> … allow the Commonwealth to consolidate and modernise its now somewhat outdated surveillance device laws …[2]

Commonwealth laws governing the use of surveillance devices for law enforcement purposes are currently found in the *Australian Federal Police Act 1979* and the *Customs Act 1901*. These laws deal only with listening devices whereas as the Second Reading Speech for the Bill points out:

> A surveillance device can be anything from an ordinary set of binoculars, a tiny microphone or camera hidden in a suspect's vehicle to a piece of software to capture the input of information to a computer.[3]

The origins of the Bill lie in the Leaders Summit on Terrorism and Multi-Jurisdictional Crime held in April 2002. The Leaders Summit 'agreed to introduce model laws for all jurisdictions and mutual recognition for a national set of powers for cross-border investigations covering controlled operations, assumed identities, electronic surveillance

devices and witness anonymity.'[4] A Joint Working Group (JWG) was established by the Standing Committee of Attorneys-General and the Australasian Police Ministers Council to prepare model legislation. The JWG produced a Discussion Paper and a Report—the latter including model legislation.[5]

The Second Reading Speech says that the Bill 'implements the electronic surveillance model Bill, tailoring it to the needs of the Commonwealth.'[6] As this suggests, there are some differences between the model Bill and the Bill before the Parliament.

The Bill does not impose a general prohibition, with exceptions, on the use of surveillance devices—in contrast to the approach taken in the *Telecommunications (Interception) Act 1979* (the TI Act). Rather, it regulates the use of surveillance devices by law enforcement agencies and the use that can be made of information collected as a result. Nor does it cover the use of surveillance devices by Australia's security and intelligence agencies. ASIO's power to obtain search warrants, computer access warrants, listening device warrants, and tracking device warrants is set out in the *Australian Security Intelligence Organisation Act 1979*. The intelligence gathering functions of the Australian Security Intelligence Service (ASIS) and the Defence Signals Directorate (DSD) are found in the *Intelligence Services Act 2001*.

Existing Commonwealth listening device, telecommunications interception and search warrant laws

Listening devices

Both the Australian Federal Police Act and the Customs Act define a 'listening device' as:

> Any instrument, device or equipment capable of being used, whether alone or in conjunction with any other instrument, device or equipment, to record or listen to spoken words.[7]

The Customs Act prohibits the use of listening devices, subject to certain exceptions. One exception is where a listening device is used under the authority of a warrant. The Customs Act enables the Australian Federal Police (AFP) and the Australian Crime Commission (ACC) to obtain listening device warrants from a judge or nominated member of the Administrative Appeals Tribunal (AAT) in order to investigate narcotics offences.

The AFP Act empowers the AFP to obtain listening device warrants in relation to persons, premises and items in order to investigate offences categorised as either 'class 1' or 'class 2' general offences. These warrants may also authorise entry onto premises. Class 1 general offences include murder, kidnapping and ancillary offences. Class 2 general offences includes certain corruption offences and perverting the course of justice offences, and offences punishable by at least 7 years in prison that involve loss of life, serious personal injury or property damage or narcotics trafficking.

Listening device warrants are issued by eligible federal Judges and certain AAT members who consider sworn information. Where such a warrant would authorise entry onto premises, additional factors need to be considered by the Judge or AAT member. For instance, in relation to class 2 general offences, the likely interference with individual privacy and the gravity of the conduct constituting the offence must be taken into account.

A listening device warrant issued under the Customs or AFP Acts can be in force for up to six months and further warrants can be issued.

Telecommunications interception

The Commonwealth does not have any general constitutional power to legislate with respect to listening or surveillance devices.[8] However, its power to legislate about telecommunications interception is not so constrained. Using its power in section 51(v) of the Constitution, the Parliament has enacted national legislation dealing with telecommunications interception—the TI Act.

The TI Act makes the interception of communications passing over a telecommunications system unlawful, subject to exceptions. One of these exceptions is interception under a law enforcement warrant. The Act enables law enforcement agencies such as the AFP, ACC and State/Territory police forces acting under a warrant to lawfully intercept such communications. There are two types of interception warrant that can be issued for law enforcement purposes—'telecommunications service' warrants and 'named persons' warrants. These warrants can also authorise entry onto premises.

For law enforcement purposes, a warrant must be obtained from an 'eligible Judge' or 'nominated AAT member'. Interception ('TI') warrants can only be issued in relation to what are called 'class 1' and 'class 2' offences. Class 1 offences include murder, kidnapping, terrorism offences and narcotics offences. Class 2 offences include offences which are, in general, punishable by at least 7 years imprisonment where the offender's conduct involves serious personal injury, drug trafficking, serious fraud, bribery or corruption. However, the 7 year threshold does not apply in all cases. For instance, recent changes inserted by the *Telecommunications (Interception) Amendment Act 2004* mean that class 2 offences include State and Territory cybercrime offences, some of which are punishable by between 1 and 5 years imprisonment.

An application for an interception warrant must be accompanied by an affidavit containing prescribed information. The TI Act also sets out the matters that the eligible Judge or nominated AAT member must consider when making a decision about whether to issue an interception warrant. These include the availability of alternative methods of investigating the offence and, in the case of class 2 offences, the gravity of the conduct under investigation and the degree that privacy will be interfered with. If the application is for a warrant authorising entry onto premises, the Judge or AAT member must also be satisfied

that it would be impracticable or inappropriate to intercept communications by less intrusive means.

TI warrants can be in force for up to 90 days and can be renewed.

The TI Act contains a variety of record keeping requirements and accountability measures. For instance, it empowers the Ombudsman to inspect records that the AFP and ACC are required to keep about interceptions and the use of intercepted information. The Ombudsman must report to the Minister about these inspections. Reports by law enforcement agencies must also be made to the Minister and there are annual reporting to Parliament requirements.

Commonwealth law enforcement and surveillance devices

Given that Commonwealth surveillance device laws deal only with listening devices, what happens if a Commonwealth law enforcement officer wishes to use a surveillance device that is not a listening device? As the JWG Discussion Paper explains:

> … if there is no relevant Commonwealth legislation [such as the Telecommunications Interception Act 1970, the AFP Act or the Customs Act], the AFP must abide by any relevant State or Territory law and the common law when using surveillance devices. However, unlike the local police force, the AFP is not able to utilise State or Territory warrant regimes. For example, if the AFP wanted to use an optical surveillance device to investigate a Commonwealth offence, the use of the device would either be permitted or prohibited by the relevant local law or otherwise subject to the common law, because there is no Commonwealth legislation regulating the use of such devices.[9]

A summary of State and Territory surveillance device laws is found in Appendix B of the JWG Discussion Paper on *Cross-Border Investigative Powers for Law Enforcement*.[10]

Crimes Act 1914

Other investigative tools are found in the Crimes Act, which enables law enforcement officers to conduct controlled operations and use assumed identities. It also enables them to obtain search warrants. Ordinary search warrants enable premises to be searched for evidential material.

In 2001, the Crimes Act was amended by the *Cybercrime Act 2001* to enable the police to 'operate electronic equipment at the warrant premises to access data (including data not held at the premises)'[11] and to copy any data that might be evidential material to disks or tapes. These powers are wider than the powers granted under an ordinary search warrant because they allow material to be seized which is unrelated to the investigation at hand.[12]

Search warrants can be obtained from a magistrate or justice of the peace who considers a sworn affidavit. A search warrant can be in force for up to 7 days.

Recovery orders

It is also notable that the Bill establishes a statutory scheme which enables surveillance devices to be used when a child recovery order has been made under the Family Law Act. Recovery orders can deal with a range of matters such as requiring a child to be returned to the child's parent or a person with a residence or contact order.

Main Provisions

Definitions

Clause 6 is the definitions provision. It defines 'surveillance device' as:

- a data surveillance device, a listening device, an optical surveillance device or a tracking device
- a device that combines two or more of those devices (ie a composite device); or
- a device prescribed by regulation.

Definitions are also provided for the different types of surveillance device:

- a 'data surveillance device' is a device or program that can record or monitor the input or output of information to or from a computer. It does not include an optical surveillance device
- a 'listening device' is a device that can be used to listen to or record a conversation or words. Devices (like hearing aids) used by those with hearing difficulties are excluded from the definition
- an 'optical surveillance device' is a device capable of visually recording or observing an activity. The definition encompasses equipment that is used only for observational purposes (like binoculars) as well as recording equipment (like cameras and video recorders). It does not include devices (like spectacles or contact lenses) that are used by the visually impaired; and
- a 'tracking device' is an electronic device capable of detecting or monitoring a person or object. It emits a radio signal that allows the movement of vehicles or objects to be monitored.[13]

Surveillance device warrants

Types of surveillance device warrant

The Bill creates two types of warrant—surveillance device warrants and retrieval warrants (**clause 10**). Different statutory regimes apply to each type of warrant.

Who can apply for surveillance device warrants?

Commonwealth, State or Territory police, Australian Crime Commission staff and secondees working for these organisations can apply for surveillance device warrants (**clauses 6 and 14**).

However, unless State and Territory police are investigating a Commonwealth offence or acting in relation to a child recovery order they must act under State or Territory laws governing surveillance device warrants [**subclause 14(2)**].[14] Similar provisions are inserted in relation to certain emergency authorisations [**subclause 28(2)**] and the use of certain surveillance devices without a warrant [**subclauses 37(2), 38(2) and 39(2)**].

When can an application be made for a surveillance device warrant?

There are two situations in which an application for a surveillance device warrant can be made.

Investigating a relevant offence

An application can be made where a law enforcement officer suspects on reasonable grounds that a 'relevant offence' has been or may be committed and that an investigation is being, will be or is likely to be conducted and that the use of a surveillance device is necessary to obtain evidence [**subclause 14(1)**].

A 'relevant offence' includes Commonwealth offences punishable by at least three years imprisonment, 'State offences that have a federal aspect' punishable by at least three years imprisonment, and offences prescribed by regulation (**clause 6**). 'Relevant offences' also include certain offences under the *Financial Transactions Reports Act 1988* and the *Fisheries Management Act 1991*.

Child recovery orders

An application can be also made where a recovery order is in force for a child and the law enforcement officer suspects on reasonable grounds that the use of a surveillance device may assist in the location and safe recovery of that child [**subclause 14(3)**].

Who can issue surveillance device warrants?

Either an eligible federal Judge or certain nominated AAT members can issue warrants. For constitutional reasons, a Judge must first consent to being declared an 'eligible Judge' and the power to issue warrants is conferred on the Judge in their personal capacity (**clauses 11-13**).

AAT members who can issue warrants are Deputy Presidents, full-time senior members, part-time senior members and ordinary members. Part-time senior members and ordinary members must be lawyers of at least five years standing.

What must an application contain and be accompanied by?

An application for a surveillance device warrant must contain:

- the name of the applicant
- the nature and duration of the warrant sought; and
- the kind of surveillance devices that the applicant wants to use [**subclause 14(5)**].

In general, the application must be accompanied by an affidavit setting out the grounds on which the warrant is sought [**paragraph 14(5)(b)**]. However, an unsworn application may be made if immediate use of the device is required and it is impracticable for the affidavit to be prepared or sworn before the application is made. In such a case an affidavit must be provided within 72 hours after the warrant application is made [**subclauses 15(6) & (7)**]. It should be noted that **clause 20** gives the Judge or AAT member the power to revoke a warrant. This power would include the power to revoke a warrant issued after an unsworn application is made.

There is also provision for remote applications ie applications made by telephone, fax, email or any other means of communication (**clause 15**).

Determining a warrant application

Subclause 16(1) provides that an eligible Judge or nominated AAT member may issue a surveillance device warrant if satisfied:

- in the case of a 'relevant offence' warrant application—that there are reasonable grounds for the suspicion on which the application is based
- in the case of a 'recovery order' warrant application—that a recovery order is in force and that there are reasonable grounds for the suspicion on which the application is based

- in the case of an unsworn application—that it would have been impracticable for the affidavit to be sworn before the application was made; and

- in the case of a remote application—that it would have been impracticable for the application to be made in person.

In deciding whether to issue the warrant, the eligible Judge or nominated AAT member must take account of a number of factors including:

- in the case of a 'relevant offence' warrant—the nature and gravity of the alleged offence

- in the case of a 'recovery order' warrant—the circumstances that resulted in the recovery order being made

- privacy issues

- alternative means of obtaining the evidence or information. The JWG model Bill also required the issuing officer to have regard to the extent to which such alternative means might assist or prejudice the investigation. In other words, the question of alternative means would be put in some sort of context. The Bill before the Parliament does not follow the model Bill in this regard

- the likely evidentiary or intelligence value of the evidence or information sought; and

- previous surveillance device warrants sought or issued that were connected with the same alleged offence or recovery order [**subclause 16(2)**].

However, unlike the regime set out in the TI Act, there is no requirement for the Judge or AAT member to take account of how any information obtained from previous warrants was used. Nor does information need to be provided to the Judge or AAT member about previous emergency authorisations or about the use of surveillance devices under **proposed Part 4** (which enables some devices to be used without a warrant or authorisation).

What must a surveillance device warrant contain?

Among the matters that must be stated in the warrant are the name and signature of the person issuing the warrant; the applicant's name; the alleged offence that the warrant relates to (or the child recovery order); the date of the warrant; the surveillance devices and premises, objects or people it covers; its duration; the name of the executing officer and any conditions that the warrant is subject to [**subclause 17(1)**].

What does a surveillance device warrant authorise?

A surveillance device warrant may authorise a surveillance device to be used in relation to one or more of the following:

- on specified premises
- in or on a specified object or class of object; and
- in respect of conversations, activities or locations of a specified person or a person whose identity is unknown [**subclause 18(1)**].

The surveillance device warrant will also authorise other activities including:

- retrieval of the device
- installation, use, maintenance and retrieval of 'enhancement' equipment[15]
- the connection of the device or enhancement equipment to 'any object or system that may be used to transmit information'
- forcible entry onto premises—including adjoining premises—so that the device can be installed, used or maintained
- the removal of objects or vehicles from premises in order to install etc the surveillance device or enhancement equipment and the return of those objects or vehicles
- breaking open things so that the surveillance device or enhancement equipment can be installed etc; and
- the provision of expert assistance to the law enforcement officer named in the warrant so that the surveillance device or enhancement equipment can be installed etc [**subclauses 18(2) & (3)**].

Other matters that the surveillance device warrant may authorise include:

- doing anything reasonably necessary to conceal the fact that a device or enhancement equipment has been installed etc [**subclause 18(4)**]; and
- interfering with the property of a person who is not the subject of the investigation—but only if the eligible Judge or AAT member issuing the warrant is satisfied that this is necessary to give effect to the warrant [**subclause 18(5)**].

A surveillance device warrant cannot authorise the doing of anything for which a telecommunications interception warrant would be required [**subclause 18(7)**].

Extending and varying surveillance device warrants

Clause 17 provides that the maximum duration of a warrant is 90 days (subject to extensions that can be granted under **clause 19**).

Clause 19 enables an application to be made for the extension of a surveillance device warrant for up to 90 days. Applications to vary the terms of the original warrant can also be made. The same matters need to be made out and the Judge or AAT member needs to be satisfied of the same things as when the original warrant application was made.

There is no limit to the number of extension and variation applications that can be made. Each extension may be for up to 90 days.

Revoking surveillance device warrants

Surveillance device warrants may be revoked in two ways:

- on the initiative of an eligible Judge or nominated AAT member; or
- by the chief officer of the relevant law enforcement agency. The chief officer must revoke the warrant if satisfied that the use of a surveillance device is no longer necessary (**clause 20**).

If a warrant is revoked by a Judge or AAT member, a written copy of the revocation must be given to the chief officer of the relevant law enforcement agency. A law enforcement officer who is executing a warrant that is revoked by an eligible Judge or nominated AAT member will not be civilly or criminally liable for anything done before he or she is made aware of the revocation [**subclause 20(5)**].

Discontinuing use of a surveillance device warrant

Clause 21 provides that if the chief officer of a law enforcement agency is satisfied that a surveillance device warrant is no longer necessary for the purposes of criminal investigation or the location and recovery of a child, then in addition to revoking the warrant under **clause 20**, he or she must take action so that the use of surveillance device is discontinued.

If the chief officer is notified by an eligible Judge or AAT member that the warrant has been revoked, the chief officer must take action so that use of the surveillance device is discontinued 'as soon as practicable'.

The Bill also requires the law enforcement officer executing the warrant to advise the chief officer of his or her agency 'immediately' if he or she believes the use of a surveillance device is no longer necessary [**subclause 21(5)**].

Retrieval warrants

Applying for a retrieval warrant

In addition to surveillance device warrants, the Bill also creates a type of warrant called a retrieval warrant. The Explanatory Memorandum explains:

> Where a SD has expired before an LEO has been able to remove the device that was lawfully installed, clause 22 allows the LEO to apply to an eligible Judge or nominated AAT member for a warrant to retrieve the SD, however such an application is not mandatory. This means, for example, that where retrieving the SD presents a disproportional cost to the LEA or some danger to the retrieval team, the SD can remain in place but cannot be used.[16]

A law enforcement officer can apply for a retrieval warrant if the officer suspects on reasonable grounds that a lawfully installed device is still on the premises [**subclause 22(1)**].

The application must be made to an eligible Judge or nominated AAT member [**subclause 22(2)**]. It must, in general, be supported by an affidavit setting out the grounds on which the warrant is sought. However, like a surveillance device warrant, a retrieval warrant may be applied for remotely or in the absence of a sworn affidavit [**subclause 22(4) and clause 23**]. A sworn affidavit must be provided within 72 hours if it does not accompany the retrieval warrant application [**subclause 22(5)**].

Determining a retrieval warrant application

An eligible Judge or nominated AAT member may issue a retrieval warrant if satisfied that there are reasonable grounds for the suspicion founding the application. He or she must also take account of privacy issues and the public interest in retrieving the device (**clause 24**). Additionally, if the application is not accompanied by an affidavit or is made remotely, the Judge or AAT member must consider whether it would have been practical for the law enforcement officer to comply with such conditions.

What must a retrieval warrant contain?

A retrieval warrant must contain the name and signature of the person issuing the warrant, the name of the applicant, the date of issue, the kind of surveillance device to be retrieved and its location, the duration of the warrant (not more than 90 days), the name of the executing officer and any conditions that attach to the warrant (**clause 25**).

What does a retrieval warrant authorise?

A retrieval warrant authorises:

- the retrieval of a surveillance device and any enhancement equipment
- forcible entry onto premises and adjoining premises in order to retrieve the device and the equipment
- breaking open anything to retrieve the device or equipment
- the temporary removal of a object or vehicle where the device or equipment is installed and the return of the object or vehicle; and
- the provision of expert assistance to the law enforcement officer involved [**subclause 26(1)**].

If a tracking device is the subject of a retrieval order then the device and any enhancement equipment can be activated for location and retrieval purposes, but only for those purposes [**subclause 26(2)**].

A retrieval warrant may authorise the doing of anything reasonably necessary to conceal the fact a device or equipment has been retrieved. Such an authorisation cannot extend to the use of the surveillance device for any purpose [**subclause 26(3)**].

Revoking a retrieval warrant

Like a surveillance device warrant, a retrieval warrant can be revoked on the initiative of an eligible Judge or nominated AAT member or by the chief officer of the relevant law enforcement agency [**subclauses 27(1)-(4)**].

As with surveillance device warrants, if the executing officer believes that the retrieval warrant is no longer needed, he or she must immediately inform the chief officer of the law enforcement agency [**subclause 27(5)**].

Emergency authorisations

In certain cases, a law enforcement officer can be authorised by a senior law enforcement officer to use a surveillance device without first obtaining a warrant. In general, authorising officers in the police forces are Commissioners and SES level officers who are authorised to perform this function. Authorising officers in the ACC are the organisation's CEO and SES officers authorised for this purpose by the CEO (**clause 6**).

There are three situations in which an emergency authorisation can be obtained from an

authorising officer.

Serious risk of harm to persons or property

An application can be made to an authorising officer for an emergency authorisation if a law enforcement officer reasonably suspects that:

- there is an imminent risk of serious violence to a person or substantial damage to property; and
- the use of a surveillance device is 'immediately necessary' to deal with the risk; and
- the circumstances are so serious and urgent that a surveillance device should be used; and
- it is not practicable to apply for a warrant [**subclause 28(1)**].

The application can be made orally or in writing and can be granted if the authorising officer is satisfied that there are reasonable grounds for the suspicion founding the application [**subclauses 28(3)-(4)**].

Child recovery orders

A law enforcement officer can also apply for an emergency authorisation if:

- a recovery order is in force; and
- the law enforcement officer reasonably suspects that the circumstances are so urgent that the immediate use of a surveillance device is warranted, and that it is not practicable to apply for a warrant [**subclause 29(1)**].

Once again, the application may be made orally or in writing and may be granted if the authorising officer is satisfied that a recovery order is in force and there are reasonable grounds for the suspicion on which the application is based [**subclauses 29(2)-(3)**].

Risk that evidence will be lost

An application for an emergency authorisation can be made if an investigation is being conducted into certain narcotics or terrorism offences and the law enforcement officer reasonably suspects that the use of a surveillance device is immediately necessary to prevent the loss of relevant evidence and the circumstances are so serious and urgent that the use of a surveillance device is warranted and it is not practicable to apply for a warrant [**subclause 30(1)**].

The application can be made orally or in writing and can be granted if the authorising officer is satisfied that an investigation is being conducted into a narcotics or terrorism offence and that there are reasonable grounds for the suspicion on which the application is based [**subclauses 30(3) & (4)**].

Records of emergency authorisation

An authorising officer must record applicant's name, the date and time of the authorisation and the nature of the emergency authorisation (**clause 31**).

What can be authorised by an emergency authorisation

An emergency authorisation may authorise:

- the use of a surveillance device or devices; and
- anything that could be authorised under a warrant.

However, an emergency authorisation does not authorise activities for which a TI warrant would be required (**clause 32**).

Approving the emergency authorisation

Within 2 business days of an emergency authorisation being issued the authorizing officer must ask an eligible Judge or nominated AAT member to approve the authorisation [**subclause 33(1)**]. A 'business day' means a day other than a Saturday, Sunday or public holiday in the relevant State or Territory (**clause 6**). In other words, depending on the time of year the authorisation could be in use for several days before approval need be sought.

Clause 34 sets out the matters which the eligible Judge or nominated AAT member must consider when an approval application is before him or her. In the context of the intrusive nature of surveillance, the matters include the extent to which alternative methods could have been used, how much they would have helped or prejudiced the particular law enforcement objective and whether or not it was practicable to apply for a warrant. Similar factors need to be considered when the application relates to a child recovery order.

Clause 35 enables an eligible Judge or AAT member to approve an emergency authorisation if satisfied of certain matters. For instance, in the case of an emergency authorisation given in relation to serious risks to persons or property, the authorisation may be approved if there were reasonable grounds to suspect that there was a serious risk and that using a surveillance device may have helped to reduce that risk and that it was not practicable to apply for a warrant.

If an approval is given, the eligible Judge or AAT member may issue a warrant for the continued use of the device or, if there is no further need for it, order that its use cease. If approval is not given, an order may be made for the surveillance to cease. Orders can also be made that information obtained from the use of the device be dealt with 'in a manner specified in the order, not being a manner that involves the destruction of that information.'

Use of surveillance devices without a warrant

Certain surveillance devices can be used without a warrant and, in certain cases, without being authorised by a senior law enforcement officer. These matters are dealt with in **proposed Part 4**.

Optical surveillance devices

A law enforcement officer can use an optical surveillance device without a warrant in the course of agency functions if the use of the device does not involve entry onto premises without permission (**clause 37**). As stated earlier, optical surveillance devices include observational devices like binoculars and recording devices like cameras and video recorders.

Surveillance devices used for listening or recording

A law enforcement officer can use a surveillance device without a warrant for listening or recording purposes, if the officer is acting in the course of agency functions and is participating in the conversation. An example would be where the officer is acting 'undercover' (**clause 38**).

Tracking devices

Clause 39 enables a law enforcement officer to use a tracking device without a warrant but with the written permission of an 'appropriate authorising officer' when investigating a relevant offence or in order to locate and recover a child who is the subject of a recovery order. The device may also be retrieved without a warrant [**subclause 39(6)**] if written authorisation is obtained.

However, authorisation of the use, installation or retrieval of the tracking device cannot be given if it would involve entry onto premises without permission or interference with the interior of a vehicle without permission [**subclause 39(7)**].

In order to obtain written authorisation the applicant law enforcement officer must apply orally or in writing, addressing the matters that would need to be addressed if the application were, instead, an application for a tracking device warrant [**subclause 39(8)**].

As stated above, a tracking device authorisation will not authorise all the things that could be done if a surveillance device warrant were to be obtained. For instance, it cannot be given if its use or retrieval would involve entry onto premises without permission or interference with the interior of a vehicle without permission. However, it will authorise action taken to conceal the device [**subclause 39(9)**]. It will also authorise breaking things open to retrieve the device and the temporary removal of an object or vehicle in which the device is installed so that the device can be retrieved [see **subclause 39(10)**].

'As soon as practicable' after giving the tracking device authorisation, the authorising officer must make a written record which includes certain information—such as the name of the applicant, the time and date of the authorisation, the offence being investigated (or details about the child recovery order, where relevant), where the tracking device is being used and any conditions governing the use of the tracking device (**clause 40**). How accurately this information will be recorded when authorisation requests can be made orally is a practical issue affecting accountability that Parliament may wish to consider.

Extraterritorial operation of warrants

Proposed Part 5 deals with the extraterritorial operation of warrants.

Subclause 42(1) provides that if, before a warrant is issued or approval is given for an emergency authorisation, the applicant law enforcement officer becomes aware that surveillance will be needed in a foreign country or on foreign vessels or aircraft outside the limits of the Australian territorial sea, the eligible Judge or AAT member must not issue the warrant unless satisfied that the surveillance has been agreed to by the foreign country.

Similarly, if a warrant has already been issued and it becomes apparent that surveillance in a foreign country or of foreign vessels or aircraft will be needed, the warrant will only permit such surveillance if the foreign country agrees [**subclause 42(3)**].

However, there are exceptions to these general rules. So, if:

- a foreign vessel is in waters within the outer limits of the contiguous zone[17] and suspected customs, fiscal, immigration or sanitary law offences are involved, or

- a foreign vessel is in waters within the outer limits of the contiguous zone and certain fishing offences are suspected

it will not be necessary to obtain the agreement of the foreign country for the surveillance 'while the vessel is in those waters.'

Subclause 42(8) provides for that, 'for the avoidance of doubt' it is not necessary to obtain the agreement of a foreign country if the foreign aircraft or vessel is in Australia or within the outer limits of Australia's territorial sea.

Evidence obtained from surveillance in a foreign country is inadmissible as evidence unless the court is satisfied that the surveillance was agreed to by the foreign country (**clause 43**).

Compliance and monitoring

Proposed Part 6 contains rules governing the use of information obtained from the use of surveillance devices. This information is called 'protected information.'

'Protected information' is defined in **clause 44**. Among other things, it means:

- any information obtained from the use of a surveillance device under a warrant, emergency authorisation or tracking device authorisation
- any information relating to an application for a warrant or the existence of a warrant, emergency authorisation or tracking device authorisation
- any information likely to identify a person or premises specified in a warrant, emergency authorisation or tracking device authorisation, or

The term, 'protected information' also includes any other information obtained by a law enforcement officer without the authority of a warrant, tracking device authorisation or an emergency authorisation that was later approved—but only if the information is obtained 'in contravention of the requirement for such a warrant, tracking device authorisation or emergency authorisation' [**proposed paragraph 44(1)(d)**].

Obtaining information under **proposed section 37** (use of optical surveillance devices without warrant) or under **proposed section 38** (use of surveillance devices for certain listening or recording purposes) does not require any warrant or emergency authorisation and so is not 'protected information' for the purposes of the legislation. As a result, the prohibitions and protections in **proposed Part 6** do not apply to this information.

Subclauses 45(1) & (2) create offences:

- it is an offence to intentionally use, record, communicate or publish information that is protected information if the use etc is not permitted and the person is reckless about that circumstance. The maximum penalty is 2 years imprisonment.
- there is an aggravated offence where the use etc recklessly endangers health or safety or prejudices the conduct of an investigation into a relevant offence. The maximum penalty is 10 years imprisonment.

Subclauses 45(4) & (5) contain exceptions to the general prohibitions on the use etc of protected information. For instance, the general prohibitions do not apply to protected

information obtained under a warrant, emergency authorisation or tracking device authorisation where the information:

- has been disclosed in open court proceedings lawfully
- is used to prevent or reduce the risk of serious violence or substantial property damage
- is communicated to the heads of Australia's security and intelligence agencies; or
- is communicated to a foreign country in respect of criminal proceedings [**subclause 45(4)**].

This 'protected information' can also be used or admitted into evidence if necessary:

- to investigate a 'relevant offence'[18]
- to make a decision about the prosecution of a relevant offence
- in 'relevant proceedings'[19]
- to investigate complaints against 'public officers' (ie Commonwealth, State or Territory office holders and employees) or to make decisions about the termination of their employment; or
- in order to keep the records required by **proposed Division 2**, for the purposes of Ombudsman inspections as required by the Act, or for the purposes of an investigation under the *Privacy Act 1988*.

It is important to note that 'protected information' obtained as a result of the unauthorised use of a surveillance device in circumstances where a warrant or other authorisation should have been obtained can be communicated:

- if it has been disclosed in proceedings in open court lawfully
- in order to help prevent or reduce the risk or serious violence to a person or substantial damage to property
- to Australia's intelligence agencies
- in order to investigate complaints against public officers and make decisions about the termination of their employment; or
- for the purposes of an inspection by the Ombudsman or an investigation under the Privacy Act [see **subclause 45(6)**].

Clause 46 imposes safe keeping requirements for 'protected information' on law enforcement agencies and also requires records of protected information to be destroyed if they are not likely to be required.

Clause 47 enables a person giving evidence to object to the disclosure of information that could reveal details of surveillance device technology or methods of use etc. In deciding whether to make a non-disclosure order a court must take account of whether disclosure is:

- necessary for the fair trial of the defendant; or
- in the public interest.

A court can also make a non-publication order.

Protected information held by a royal commission, court or tribunal cannot be accessed except by order of that body (**clause 48**).

Reporting and record-keeping

Proposed Part 6 of the Bill also sets out a number of reporting and record keeping requirements.

Reports on warrants and authorisations

As soon as practicable after a warrant or authorisation has expired, each law enforcement agency that has obtained a warrant or authorisation must report to the Minister and provide a copy of the warrant or the authorisation. The report must include specified information—for instance:

- whether the warrant or authorisation was executed; and
- if so, who executed the warrant, the kind of device used, the period of use, the name of anyone whose activities were monitored or recorded, details of where the device was installed, how the use of the device benefited the investigation of a relevant offence or assisted in the location and recovery of a child, and how the conditions of the warrant were complied with. Any extensions or variations of the warrant must also be stated (**clause 49**).

In the case of a retrieval warrant, the report must provide details of any premises entered in order to retrieve the warrant, whether or not the device was retrieved and information about compliance with the conditions of the warrant.

Annual reports

Law enforcement agencies must also report to the Minister within 3 months of the end of each financial year. The Minister must table the report in Parliament within 15 sitting days of receiving it (**clause 50**).

The report must satisfy statutory reporting requirements such as:

- the number of warrant and authorisation applications, the numbers issued and refused (and the reasons for refusals)
- the number of extension applications made, granted and refused (and the reasons for granting or refusing)
- the number of remote applications
- the number of arrests made 'on the basis (wholly or partly) of information obtained' by use of surveillance devices or tracking devices issued under warrant or authorisation; and
- the number of prosecutions for relevant offences commenced where information obtained from the authorised use of surveillance or tracking devices was given in evidence and the number of prosecutions that resulted in a guilty verdict.

Record-keeping requirements

Clauses 51 and 52 set out requirements for record-keeping which must be met by law enforcement agencies. For instance, law enforcement agencies must keep each warrant issued and each application made for a warrant, emergency authorisation and tracking device authorisation, records of each emergency authorisation and tracking device authorisation, and a copy of each section 49 report to the Minister.

Each law enforcement agency must also keep records containing the information required in the annual report to the Minister (see above).

Register of warrants, emergency authorisations and tracking device authorisations

Each law enforcement agency must keep a register of warrants and authorisations that contains information such as the date the instrument was issued or refused, the name of the authorising judicial officer or other person, the name of the executing officer, the relevant offence or the name of the relevant child (in relation to a recovery order) the period for which the instrument was in force and any variations or extensions of the warrant (**clause 53**).

Inspections

The Bill enables the Commonwealth Ombudsman (or his/her inspecting officers) to inspect the records of law enforcement agencies in order to determine whether statutory requirements have been met by the agency and its officers (**clause 55**). For these purposes, the Ombudsman must be given 'full and free' access to relevant agency records, may copy those records and require staff members to provide relevant information. These inspections can be carried out during the currency of a warrant or authorisation but the Ombudsman can refrain from doing so at such time if he or she so chooses [**subclause 55(4)**].

It is an offence, punishable by a custodial sentence of up to six months, to refuse to give information or answer questions if the Ombudsman requires a person to do so [**subclause 56(6**)]. **Clause 57** makes it clear that self-incrimination does not excuse a person from complying with such a requirement. However, the person is provided with a use and derivative use immunity.[20]

Clause 58 enables the Ombudsman to exchange information with State or Territory 'inspecting authorities'. These are agencies that perform similar functions under State or Territory law.

At six-monthly intervals the Ombudsman must report to the Minister on the results of each inspection.[21] The Minister must table the report in Parliament within 15 sitting days (**clause 61**).

Evidentiary certificates

Clause 62 enables law enforcement agencies to provide certificates that are prima facie evidence of what they state for the purposes of court proceedings. For example, an evidentiary certificate can state as facts anything done by a law enforcement officer when acting under a warrant, under an approved emergency authorisation or under a tracking device authorisation.

Such a certificate cannot be admitted into evidence unless the defendant has been given a copy of the certificate at least 14 days before the prosecution seeks to have it admitted into evidence.

If a certificate is admitted into evidence, the defendant can require the person who gave the certificate to appear as a witness for the prosecution and be cross-examined in court.

Schedule 1

Schedule 1 makes a number of transitional and savings amendments. For instance, it repeals those provisions in the AFP Act that currently deal with listening devices and

makes transitional and saving arrangements for listening devices warrants in force at the time of the repeal.

Concluding Comments

Privacy

Both the JWG report and the Attorney-General's Second Reading Speech note that it is important to protect society against crime and that surveillance technology can be an important weapon in the law enforcement arsenal. In view of the intrusive nature of surveillance, they also acknowledge the need to protect privacy interests. Privacy interests have been identified as being:

- the interest in controlling entry to personal territory
- the interest in freedom from interference with one's person and personal space
- the interest in controlling one's personal information; and
- the interest in freedom from surveillance and from interception of one's communications.[22]

One reason for the Bill to protect privacy interests and regulate the use of surveillance is the limited protection given by the common law when a person is subjected to surveillance.[23] In this context, it may be important to note that surveillance devices can intrude into the lives of third parties who have nothing to do with police investigations. Another reason for taking privacy issues into account is the obligations Australia has as a party to the International Covenant on Civil and Political Rights (ICCPR). Article 17 of the ICCPR provides:

> (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> (2) Everyone has the right to the protection of the law against such interference or attacks.

Various provisions in the Bill aim to address privacy issues. For instance, warrants are issued by Judges and AAT members, restrictions are placed on the uses to which 'protected information' can be put, there are record-keeping and reporting requirements, and inspection provisions. On the other hand, the Bill contains no general prohibition on the use of surveillance devices subject to exceptions. It enables surveillance devices to be used without warrant or authorisation in certain circumstances. 'Protected information'

obtained without the requisite authorisation can be used in a range of circumstances not restricted to the investigation of complaints. And information obtained lawfully without a warrant is not 'protected information' for the purposes of the legislation. These and other issues are considered in more detail below. Parliament may wish to consider whether the proposed statutory regime constitutes a reasonable and proportionate interference with privacy.[24]

The accused and a fair trial

The ICCPR also provides, in article 14, that an accused has a right to a fair trial. One of the incidents of a fair trial is the accused's right to silence.[25] Article 14(3)(g) of the ICCPR says that an accused person has the right '[n]ot to be compelled to testify against himself or to confess guilt'.

Parliament may want to consider whether the provisions in the Bill, including the uses that can be made of information obtained without the need for a warrant, are an acceptable or an unwarranted interference with an accused's right to silence.

Offence thresholds

The application of the Bill in a law enforcement context is determined by the scope of the definition of 'relevant offence' in **clause 6**.

The issue of offence thresholds was the subject of differing submissions to the JWG Discussion Paper. Privacy bodies such as Privacy NSW supported a three year threshold[26] as serving an 'important symbolic privacy function in recognising that surveillance, by its very nature, is privacy invasive and that it requires a strong public interest to overcome objections to its use.'[27] Legal bodies, such as the Law Council of Australia and the International Commission of Jurists, recommended a higher threshold of either 7 years, in line with the general scheme of the TI Act, or 10 years. The Victoria Police proposed an 'any offence' threshold.

The JWG concluded that its original proposal (for a three year threshold) should be supplemented by a provision enabling regulations to prescribe offences that fall below the three year threshold. This is the position adopted in the Bill.

Emergency authorisations

Loss of evidence

The JWG Report supported the use of emergency authorisations (ie no prior warrant) in limited circumstances—in summary, where a serious risk of personal violence or substantial property damage existed.[28] It remarked:

> The JWG believes that there are limited circumstances when it may be impracticable for law enforcement agencies to apply for a warrant, even by telephone. These are the circumstances contemplated by clause 21 [clause 28 of the Bill] (where the scale of potential harm or damage is serious and the time pressures are urgent) … The JWG considered, but rejected, singling out serious drug offences as a separate category for which emergency authorisations may be issued.[29]

In a criminal law context, the Bill adopts the JWG recommendation but also adds to it by enabling emergency authorisations to also be granted where there is a risk of loss of evidence in relation to certain offences (such as prohibited imports and narcotics offences, and terrorism offences).

Destruction of information

Both the model Bill and the Bill before the Parliament deal with what happens to information that has been collected under an emergency authorisation. The model Bill contained a clause giving a Judge considering an emergency authorisation approval application the power 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.'[30] This would have included destroying the information. However, the Bill provides that the Judge or AAT member may order that information obtained from the use of an emergency authorisation be 'dealt with in a manner specified in the order, not being a manner that involves the destruction of that information.'[31]

Parliament may wish to consider whether a Judge or AAT member should have the power to order the destruction of records. As the JWG Discussion Paper points out, this would provide:

> … an additional safeguard if the law enforcement agency obtains material that falls outside the … approval.[32]

It would also ensure that material would be destroyed where an approval was not obtained thus guaranteeing that it could not be used under any of the 'protected information' exceptions found in **clause 45**.

Using surveillance devices without a warrant or emergency authorisation

Optical surveillance devices

The Bill enables optical surveillance devices to be used without a warrant if their use does not involve entry onto premises or into vehicles without permission. The Second Reading Speech comments:

> Less intrusive surveillance may be carried out without a warrant. There is nothing unusual about this. Police, throughout our history and across jurisdictions, have engaged in certain types of surveillance without a warrant. For example, this might include the use of binoculars to watch a group of terrorists scout a location for a possible attack. This is routine police work and must not be subject to unnecessary restrictions which would destroy police effectiveness.

However, the exception relating to optical surveillance devices is not confined to observational devices like binoculars or telescopes. It includes recording devices and appears to encompass recording devices like video cameras that can capture sound as well as images. In a report published in 2001, the NSW Law Reform Commission remarked:

> … visual surveillance can be extremely invasive and can identify individuals more clearly than audio devices, leading to the comment in *R v McNamara* that "the use of a video camera … is in some respects more intrusive than a sound transmitter."[33]

Tracking devices

The JWG considered but rejected suggestions that the power to approve the use of a tracking device should be exercisable by a senior law enforcement officer rather than a judicial officer.[34] It noted:

> Given the intrusion on privacy involved in surveillance, it is necessary for an impartial authority to evaluate the application and consider whether surveillance is appropriate.[35]

The Bill takes a different approach. It provides that tracking devices can used if approved by a senior law enforcement officer, although approval cannot be given if the installation or retrieval of the device involves entry onto premises without permission or interference with the interior of a vehicle without permission.

Parliament may want to consider whether privacy interests suggest that tracking devices should be treated in the same way as other surveillance devices.

The JWG also concluded that a composite device (one with tracking and other surveillance functions) should require judicial authorisation. While the Bill contemplates that surveillance devices may be composite devices, it does not appear to require composite tracking devices to be authorised by way of warrant.

Discontinuing the use of surveillance and tracking devices and issues of timing

The Bill provides that if the chief officer of a law enforcement agency considers that a surveillance or tracking device is no longer needed, he or she must ensure that the use of the device is discontinued. The JWG proposed the chief officer should act 'as soon as practicable'.

The JWG also proposed that when the chief officer is notified that a warrant has been revoked he or she must take action to ensure that use of the surveillance device authorised by the warrant 'is discontinued immediately'. The Bill provides that the action should be taken 'as soon as practicable'. Parliament may wish to consider whether, because of the privacy issues involved in the use of surveillance devices, the words proposed by the JWG should be adopted. This may also help to ensure that devices are not used for purposes other than the purposes for which they were granted.

Communication of 'protected information'

Clause 45 contains offences relating to the use etc of 'protected information' and exceptions to the general prohibitions on its use.

If 'protected information' is collected without warrant or authorisation or where it is collected as a result of an emergency authorisation that is not subsequently approved then it cannot be used for criminal investigation purposes, for the purposes of making decisions about prosecuting a relevant offence or in evidence. However, it may be used etc in a range of other circumstances as the Explanatory Memorandum explains:

> Protected information that falls within paragraph 44(d) may still be used, recorded, communicated or published under the exceptions contained in 45(4)(a),(b),(c),(d) and (e) because of the overriding public or national security interest in each case. Similarly, such information may also be communicated under the exceptions contained in 45(5)(d),(e),(f),(g) and (h) because these exceptions allow for the investigation into any improprieties which may attach to the surveillance itself or any subsequent use of protected information which have been gathered through that surveillance.[36]

What this means is that there are two broad types of use that can be made of protected information obtained without authorisation. One is unexceptional. Use is permitted for the purposes of investigating complaints about the use of surveillance devices or the information obtained from them [see **paragraphs 45(5)(d)-(h)**].

The second category of exceptions [contained in **paragraphs 45(4)(a)-(d)**] mean that information can be used and communicated if it has been disclosed in open court 'lawfully', or it is believed that the use or communication is necessary to 'prevent or reduce the risk of serious violence to a person or substantial damage to property' or it is communicated to the head of one of Australia's intelligence agencies[37] where 'it relates or appears to relate to any matter within the functions' of that agency. It may also be used and communicated by officers of those agencies in the performance of their official functions.

The paragraph enabling 'protected information' to be communicated to the heads of Australia's intelligence agencies is widely cast. It need only relate or appear to relate to any matter within an agency's functions. It is not confined to the communication of

information about activities that are prejudicial to national security. The JWG took a different approach to that employed in the Bill. Its model bill provided that protected information could not be communicated to ASIO if it had been collected under an emergency authorisation that was not subsequently approved.

Finally, questions might be asked about paragraph (c) of the definition of 'protected information'. This provision has clearly been formulated with privacy issues in mind. For example, 'protected information' includes information likely to identify a person, object or premises specified in a warrant, emergency authorisation or tracking device authorisation. However, the definition also encompasses any information relating to the existence of a warrant, emergency authorisation or tracking device authorisation.[38] The publication of such information[39] is an offence carrying a penalty of up to two years imprisonment. A person need not intend any adverse consequences to privacy or law enforcement activities. Nor is the offence related only to the currency of the warrant or a limited period thereafter. Parliament may wish to consider whether such a provision places undue restrictions on public debate about the use of surveillance devices by law enforcement officials.

Information that is not 'protected information'

As discussed in the Main Provisions section of this Digest, certain information obtained from the use of surveillance devices does not fall within the definition of 'protected information' at all. This means that it is not subject to the prohibitions and restrictions placed on the use of 'protected information' that are found in **proposed Part 6**. For example, use of an 'optical surveillance device' by a law enforcement officer in the course of their duty does not require a warrant or other authorisation. Nor does use of a surveillance device for listening or recording in certain circumstances. As a result, information obtained from such surveillance devices is not 'protected information' because it is not information obtained in contravention of a requirement for a warrant or authorisation. Thus, it will not be an offence to use, communicate or publish such information. And it can be admitted into evidence in any proceedings, communicated to intelligence agencies for any purpose, etc.

Parliament may want to consider whether or not it is appropriate for the use of such information to be outside the prohibitions and protections contained in **proposed Part 6**.

'Front end' accountability

One of the issues raised in submissions to the JWC was whether there should be additional 'front end' accountability for surveillance device warrants. One of the 'front end' accountability provisions in Queensland law is the Public Interest Monitor (PIM). The PIM:

> … monitors compliance by police officers with the legislation when they apply for surveillance device warrants, appears at hearings for surveillance device warrants to

> test the validity of the application, gathers statistical information about the use and effectiveness of warrants, reports to the Commissioner on non-compliance by police officers, and reports annually to the Minister.[40]

Some submissions to the JWG supported the use of an independent officer to attend hearings and review performance. Others did not. The JWG came to the view that judicial scrutiny of warrant applications provided sufficient front end scrutiny.

Computers, interception, surveillance and search warrants

If the Bill is passed, it appears that there will be a more complex scheme than already exists governing access to people's computers and their emails.

The JWG considered suggestions that the 'definition of data surveillance should be expanded to protect stored email messages and internet browsing logs'.[41] It rejected such suggestions on the basis that this information 'should arguably be captured by the ordinary search warrant process' and that … 'reform in [the area of unread emails], whether through the TI Act or other regulation is beyond the scope of this project.'[42]

The Telecommunications (Interception) Amendment Bill 2004, which was recently before the Parliament, was designed to reform the law relating to stored or delayed access communications like emails, text messages and voicemail. The Bill was referred to the Senate Legal and Constitutional Legislation Committee, which heard evidence from the Australian Federal Police and the Attorney-General's Department. This evidence revealed differences of opinion about the operation and interaction of the TI warrant regime and section 3L of the Crimes Act (the regime that deals with search warrants and computers).

The AFP had legal advice from the Director of Public Prosecutions that section 3L permits it to remotely access both read and unread emails from a computer when it is acting under an ordinary search warrant. The Attorney-General's Department disagreed and referred to advice from the Solicitor-General that a TI warrant would be required for such activity.[43]

A question that could arise is whether the Surveillance Devices Bill may add to this confusion. The definition of 'surveillance device' in the Bill includes 'data surveillance devices'. These are devices or programs 'capable of being used to record or monitor the input of information into or the output of information from a computer …[not including optical surveillance devices].' The JWG report points to the usefulness of data surveillance devices from a law enforcement perspective:

> … with the increasing adoption of encryption technology it is desirable for law enforcement to be able to monitor computer activity prior to material becoming encrypted or after it has been decrypted. … the ability to monitor the input of information as it is typed into the computer allows the police to record the information before it is encrypted. The surveillance of computer output, such as images on a monitor, can also be used to overcome difficulties with encryption.[44]

Questions might arise about what sort of warrant is needed in relation to email—for example, depending on whether the email is being typed into a computer or has been read or not read by its intended recipient. And while the Bill provides that certain types of surveillance cannot be carried out under its auspices if a TI warrant would be 'required', it may not be clear—as the dispute between the AFP and the Attorney-General's Department indicates—whether a TI warrant is required in a particular case. Nor is it clear that in any case where a warrant is needed it should be the most privacy protective warrant that is required.

Surveillance and interception

If the Bill is passed it will add to the number of different warrants that are available under different statutes covering similar situations. There will also be new categories of information and associated rules for using and communicating it (for instance, three categories of information under the Bill[45] in addition to information covered by Part VII of the TI Act[46]). There are also different accountability regimes under the Bill and the TI Act. Further, entirely different rules apply to search warrants under section 3L of the Crimes Act.

Parliament may wish to consider whether this combination fragmentation and complexity will create unacceptable difficulties for both law enforcement agencies and people who are placed under surveillance, whose telecommunications are intercepted and whose computers may be accessed.

Endnotes

1 See the definition in clause 7 of the Bill.

2 Attorney-General, Second Reading Speech, 'Surveillance Devices Bill 2004', House of Representatives, *Hansard*, 24 March 2004, p. 27010.

3 ibid.

4 Standing Committee of Attorneys-General and Australasian Police Ministers Council Joint Working Group on National Investigation Powers (JWG), *Cross-Border Investigative Powers for Law Enforcement, Discussion Paper*, February 2003, p. i.

5 See JWG, Discussion Paper, op. cit & JWG, *Cross-Border Investigative Powers for Law Enforcement. Report*, November 2003.

6 Attorney-General, Second Reading Speech, 'Surveillance Devices Bill 2004', House of Representatives, *Hansard*, 24 March 2004, p. 27010.

7 Section 12, AFP Act; section 219A, Customs Act.

8 The constitutional underpinnings of Commonwealth listening or surveillance device laws are the Commonwealth's power to make laws about offences and criminal investigation that are incidental to particular heads of power—like the power over trade and commerce with other countries or powers over taxation or external affairs.

9 JWG, Discussion Paper, op. cit, p. 203.

10 February 2003.

11 Subsection 3L(1).

12 Simon Bronitt & Miriam Gani, 'Shifting boundaries of cybercrime: from computer hacking to cyber-terrorism', (2003) 27 *Criminal Law Journal*, pp. 303–21 at p. 315.

13 JWG, Report, op. cit.

14 In other words, in relation to the investigation of State offences with a federal aspect and State offences without a federal aspect, State and Territory police must act under State or Territory laws rather than under the Commonwealth's surveillance devices legislation.

15 'Enhancement equipment' means 'equipment capable of enhancing a signal, image or other information obtained by the use of the surveillance device' (clause 6).

16 p. 15.

17 This term is defined in the *Seas and Submerged Lands Act 1973*.

18 A term defined in clause 6.

19 A term defined in clause 6. It includes the prosecution of a 'relevant offence', proceedings for the confiscation or forfeiture of property, proceedings for the protection of a child or intellectually impaired person, proceedings concerning the validity of a warrant or authorisation, disciplinary proceedings against public officers, coronial inquests, International Criminal Court proceedings, and bail proceedings.

20 This is the most comprehensive kind of immunity available to a witness. First, it prevents direct use of a witness's testimony against him or her. Second, it prevents anything obtained or derived indirectly from the witness's testimony being used against him or her.

21 The Bill refers to inspections carried out under clause 54. This appears to be a drafting error. Clause 55 is the relevant provision.

22 Australian Law Reform Commission, *Privacy*, Report No. 22, 1983, para. 46.

23 See the discussion in JWG, Report, op. cit, and in NSWLRC, op. cit.

24 See Simon Bronitt, 'Electronic surveillance, human rights and criminal justice', (1997) 3(2) *Australian Journal of Human Rights*, pp. 183–208.

25 See the discussion in Bronitt, op. cit.

26 That is, offences punishable by at least three years imprisonment.

27 JWG, Report, op. cit, p. 385.

28 The model Bill proposed by JWG would also have allowed for emergency authorisation to protect evidence when an investigation became a cross-border investigation but where

surveillance had already been occurring under a State or Territory law, generally based on a judicial warrant.

29 JWG, Report, op. cit, p. 435.

30 Ibid., p. 446.

31 Subclause 35(6).

32 JWG, Discussion Paper, op. cit, p. 293.

33 New South Wales Law Reform Commission (NSWLRC), *Surveillance: An Interim Report*, Report No. 98, 2001, p. 43.

34 ibid, p. 377.

35 ibid, p. 381.

36 Explanatory Memorandum, pp. 33–4.

37 ASIO, ASIS or DSD.

38 A prohibition on the publication of 'designated warrant information' is found in the TI Act (section 63). 'Designated warrant information' includes information about the existence or non-existence of a TI warrant (section 6EA).

39 If the requisite fault elements are proved.

40 JWG, Report, op. cit, p. 389.

41 Ibid., p. 347.

42 Ibid., p. 348.

43 See: Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2004*, March 2004. As a result of the Committee's report the Bill was split and the disputed provisions are not contained in the legislation that was passed [the *Telecommunications (Interception) Amendment Act 2004*].

44 JWG, Report, op. cit, p. 215.

45 'Protected information' that is lawfully obtained; 'protected information' not obtained by warrant or authorisation when this is required; and information that is not 'protected information.'

46 Part VII of the TI Act covers dealings in intercepted information.