Department of the Parliamentary Library

INFORMATION AND RESEARCH SERVICES

Bills Digest

No. 121 2001–02

Telecommunications Interception Legislation Amendment Bill 2002

ISSN 1328-8091

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 Department of the Parliamentary Library can be found at:
http://www.aph.gov.au/library/

Published by the Department of the Parliamentary Library, 2002

INFORMATION AND RESEARCH SERVICES

Bills Digest
No. 121 2001–02

Telecommunications Interception Legislation Amendment Bill 2002

Jennifer Norberry & Katrine Del Villar
Law and Bills Digest Group
15 April 2002

Contents

Telecommunications Interception Legislation Amendment Bill 2002

Date Introduced: 12 March 2002

House: House of Representatives

Portfolio: Attorney-General

Commencement: Most of the amendments commence on Royal Assent. Others, designed to cure drafting errors in the *Telecommunications (Interception) Legislation Amendment Act 2000,* are retrospective to 22 June 2000, the date on which that Act commenced.

Purpose

To amend the *Telecommunications (Interception) Act 1979* (the Principal Act) to:

- permit telecommunications intercept warrants to be obtained to investigate offences of terrorism, serious arson and child pornography
- stipulate when services such as emails and voicemails will come within the ambit of the Principal Act
- enable intercepted information to be passed on, for certain purposes, to the NSW Independent Commission Against Corruption (ICAC), WA Anti-Corruption Commission, the WA Royal Commission into Police Corruption, and in connection with decisions to terminate the appointment of police officers
- give certain powers to senior executive officers at the NSW Independent Commission Against Corruption (ICAC), which may currently only be exercised by the Commissioner or Assistant Commissioner
- clarify that warrants authorising entry onto premises are distinct from telecommunications service warrants and named persons warrants, and
- make other miscellaneous amendments, including the removal of references to defunct State bodies such as the Queensland Criminal Justice Commission (CJC) and the substitution of references to its replacement body, the Crime and Misconduct Commission (CMC).

The Bill also amends the *Customs Act 1901* so that Federal Magistrates and Family Court judges as well as Federal Court judges can issue listening device warrants under that Act.

Background

Telecommunications Interception Legislation Amendment Bill 2001

On 27 September 2001, the Telecommunications Interception Legislation Amendment Bill 2001 (the 2001 Bill) was introduced into the House of Representatives. However, it had not passed either Chamber before the Parliament was prorogued for the 2001 General Election and, consequently, it lapsed.

The 2002 Bill is substantially the same as the 2001 Bill. In brief, the major differences are:

- the addition of terrorist acts as offences that can be investigated by means of a telecommunications interception warrant
- the inclusion of new provisions that stipulate when a 'delayed access message service' such as an email or voicemail will come within the ambit of the Principal Act
- the inclusion of an existing State body, the ICAC, and a new State body, the Western Australian Royal Commission into Police Corruption, as bodies that can receive lawfully intercepted information from an intercepting agency when that information relates to their investigations
- the removal of references to defunct State bodies such as the CJC, the substitution of the names of replacement bodies and consequential changes.

Telecommunications interception

Prior to the commencement of the *Telephonic Communications Act 1960* (Cwlth) there were no statutory prohibitions on telephone interception in Australia. The 1960 Act prohibited telephone interception except in very limited circumstances. Interceptions could only be carried out for national security reasons or by the Postmaster-General's Department for technical purposes or to trace unlawful calls (eg nuisance calls). Interception for general law enforcement purposes was not permitted. The use of telephone intercepts for general law enforcement purposes 'lacked a secure legal basis until the enactment of the [Principal Act].[1]

As originally enacted, the Principal Act enabled interception warrants to be granted for the investigation of narcotics offences under the *Customs Act 1901*. Since 1979, the offences that can be investigated under an interception warrant have multiplied and the number of

agencies authorised to apply for interception warrants has increased. The purposes for which intercepted material can be used have also been broadened.

The Principal Act prohibits the interception of 'a communication passing over a telecommunications system' except in specified circumstances.[2] In general, these are in order to operate or maintain the telecommunications system or pursuant to a warrant.[3]

How is 'interception of a communication' defined?

Section 6 of the Principal Act defines the expression 'interception of a communication' in the following way:

> … interception of a communication passing over a telecommunications system consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication.[4]

The words, 'passing over', include 'being carried'.[5]

Types of interception warrant

Warrants may be obtained in relation to a particular identified telecommunications service ('telecommunications service warrants'), or any telecommunication service that is used or likely to be used by a named individual ('named person warrants'). An application for an interception warrant can include a request that the warrant authorise entry on to specified premises.

The Principal Act stipulates the purposes for which interception warrants may be obtained, who can apply for and issue such warrants, the form and content of warrant applications, the criteria that must be satisfied before warrants can be issued, the scope of warrants and record keeping and reporting requirements.

Who issues interception warrants and what are the purposes for which such warrants can be obtained?

Under the Principal Act warrants can be obtained for two purposes. The first is for security and intelligence. The second is for law enforcement.

Security and intelligence

The Attorney-General may issue warrants for the interception of telecommunications where the subject of the warrant is reasonably suspected of engaging in activities prejudicial to security.[6] He or she may also issue interception warrants for the collection of foreign intelligence.[7]

In certain circumstances, ASIO's Director-General of Security may issue a warrant for a limited period if waiting for a response from the Attorney-General would seriously prejudice national security.[8]

Law enforcement

Where a law enforcement agency wishes to obtain an interception warrant, an application must be made to an 'eligible judge' or nominated member of the Administrative Appeals Tribunal (AAT).[9]

Interception warrants can only be issued in relation to the investigation of what are called class 1 and class 2 offences. Class 1 offences include murder, kidnapping, and narcotics offences.[10] Class 2 offences include offences punishable by imprisonment for life or a period of at least 7 years where the offender's conduct involves serious personal injury, drug trafficking or serious fraud, bribery or corruption.[11]

Who may apply for an interception warrant?

ASIO's Director-General of Security may apply for an interception warrant relating to national security or foreign intelligence.[12]

The following agencies can apply for and obtain interception warrants for the purpose of law enforcement:[13]

- the Australian Federal Police,
- the National Crime Authority, and
- an 'eligible authority' of a State or the Northern Territory[14] in respect of which a Ministerial declaration is in force.[15] As at 30 June 2000, Ministerial declarations were in force for the Victorian, NSW, South Australian and Western Australian police services, the NSW Crime Commission, the NSW Independent Commission Against Corruption (ICAC) and the NSW Police Integrity Commission.[16]

Ministerial declarations are disallowable instruments under the Principal Act.[17]

Some other agencies that are 'eligible authorities' under the Principal Act but for whom no Ministerial declaration is in force can obtain lawfully intercepted information from intercepting agencies when that information relates to their own investigations.[18]

Criteria that must be satisfied before a warrant can be issued

An application by a law enforcement agency for an interception warrant must be accompanied by an affidavit containing prescribed information.[19] Further, before issuing an interception warrant the eligible judge or nominated AAT member must be satisfied of the matters set out in the Principal Act.[20] There are differences between telecommunications service warrants and named person warrants. There are also

differences in the statutory prerequisites for issuing warrants for class 1 and class 2 offences. Thus, before issuing a warrant in the case of a class 2 offence, the Judge or AAT member must consider the gravity of the offence and how much the privacy of any person or persons would be interfered with as a result of the warrant application being granted. Further, additional information must be supplied before a warrant can authorise entry on to premises.

When can intercepted information be used and by whom?

Subject to certain exemptions, information lawfully gathered by a telecommunications intercept may not be communicated to another person[21] or given in evidence in legal proceedings.[22] Some of the exceptions are set out below.

Exempt proceedings

Section 74 of the Principal Act expressly permits lawfully obtained information to be given in evidence in an 'exempt proceeding'. There is a wide range of '*exempt proceedings*',[23] including:

- prosecutions for 'prescribed offences' (including class 1 offences, class 2 offences and offences punishable by life imprisonment or imprisonment for three years[24])
- proceedings for confiscation or forfeiture of property
- certain extradition proceedings
- police disciplinary proceedings
- other proceedings relating to misbehaviour by Commonwealth or State officers
- bail applications relating to a prosecution for a prescribed offence
- coronial inquests examining an event that may have been caused by the commission of a prescribed offence
- proceedings of the Australian Federal Police, the National Crime Authority, the Royal Commission into the NSW Police Service, or the NSW Police Integrity Commission, and
- applications for restraining orders preventing the disposal of property pending the outcome of proceedings connected to the commission of a prescribed offence.

Permitted purposes

In addition, section 67 permits intercepted information to be communicated to another person for a '*permitted purpose*'. Those purposes which are permitted include purposes connected with:[25]

- investigations into 'prescribed offences'
- decisions whether or not to institute, and the conduct of, 'relevant proceedings'[26]
- investigations into and reporting on alleged misbehaviour or improper conduct by a Commonwealth or State public servant (including advice to terminate his or her employment)
- Commonwealth Royal Commission investigations and reports
- investigations and reports by the NSW Police Integrity Commission of police misconduct, (including advice to terminate a police officer's employment based on misconduct), and
- decisions relating to the engagement, retirement or termination of the employment of Australian Federal Police officers.

Other circumstances in which disclosure is permitted.

There are further exceptions which permit disclosure by particular persons in defined circumstances, including the interceptor,[27] the chief officer of an agency,[28] and members of the police force.[29]

Thus, under section 68 of the Principal Act, the chief officer of an intercepting agency can disclose intercepted information to certain specified agencies when that information is relevant to their investigations.[30] This is so whether or not a Ministerial declaration is in force for that agency. These agencies include the police services of the Commonwealth, each State and the Northern Territory, the National Crime Authority, the Royal Commission into the NSW Police Service, the NSW Police Integrity Commission, the Inspector of the Police Integrity Commission, the Queensland Crime Commission (QCC) and the Western Australian Anti-Corruption Commission.[31]

Certifying officers

The Principal Act creates the position of 'certifying officer'. 'Certifying officers' have a number of powers including:

- the power (if such power is delegated by the chief officer of the agency) to revoke a warrant which remains in force, if the grounds on which the warrant was issued no longer exist[32]
- the power to certify a true copy of an interception warrant which is to be provided to a telecommunications carrier[33]
- the power to certify a true copy of an interception warrant which can be received as evidence in court proceedings[34], and

- the power to issue an evidentiary certificate setting out facts relating to the execution of an interception warrant and the use made of intercepted information, which can be received as evidence in court proceedings.[35]

The Principal Act designates a range of senior executive officers of agencies including the Australian Federal Police, the National Crime Authority, the police services of each State and the Northern Territory, and various State investigative bodies to be 'certifying officers'. These State investigative bodies include the NSW Police Integrity Commission and the WA Anti-Corruption Commission.

The Government's package of counter-terrorism Bills

The Bill is effectively part of a package of counter-terrorism legislation introduced by the Howard Government on 12 March 2002. The other Bills in the package are the Security Legislation Amendment (Terrorism) Bill 2002 [No.2][36], the Criminal Code Amendment (Suppression of Terrorist Bombings) Bill 2002, the Suppression of the Financing of Terrorism Bill 2002, and the Border Security Legislation Amendment Bill 2002. Other components of the anti-terrorism package are the *Criminal Code Amendment (Anti-hoax and Other Measures) Act 2002* and the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002 (the ASIO Bill).[37] The ASIO Bill has been referred to the Parliamentary Joint Committee on ASIO, ASIS and DSD for report by 3 May 2002. The other five Bills[38] have been referred to the Senate Legal and Constitutional Legislation Committee for report by the same date.

Readers of this Digest are referred to the Digests that have been or will be produced for each of these Bills and to two Parliamentary Library Research Papers, Terrorism in Australia: Legislation, Commentary and Constraints and Terrorism and the Law in Australia: Supporting Materials.

The two Research Papers contain a detailed treatment of issues associated with legislating to counter terrorism. One relevant theme struck in those papers is that in enacting specific anti-terrorism laws a cautious and considered approach must be taken. If there was a thesis in the *Terrorism and the Law in Australia* project it was that there are dangers in *under*estimating our legislative and administrative preparedness and that there are difficulties in striking an appropriate balance between safety and liberty. The question of preparedness and the difficulty of balancing safety and liberty are considered in the *Legislation, Commentary and Constraints* Paper. Comparative approaches in the United Kingdom and United States are canvassed in the *Supporting Materials* Paper. In summary, the Paper observes that while precedents are useful, we will need our own views regarding the terrorist threat in Australia and whether the measures in question are necessary, sufficient and proportionate.

Also of note is the recent Leader's Summit on Terrorism and Multi-Jurisdictional Crime. On 5 April 2002, the Prime Minister and State and Territory Leaders negotiated an

Agreement on Terrorism and Multi-Jurisdictional Crime. In relation to terrorism, this included an agreement to:

> … take whatever action is necessary to ensure that terrorists can be prosecuted under the criminal law, including a reference of power of specific, jointly agreed legislation, including roll back provisions to ensure that the new Commonwealth law does not override State law where that is not intended and to come into effect by 31 October 2002. The Commonwealth will have power to amend the new Commonwealth legislation in accordance with provisions similar to those which apply under Corporations arrangements. Any amendment based on the referred power will require consultation with and agreement of States and Territories, and this requirement to be contained in legislation.[39]

At present, the details and implications of the Agreement are not clear.

Main Provisions

Schedule 1—Miscellaneous amendments

Categories of offence

As described above, interception warrants may only be issued in connection with the investigation of 'class 1' or 'class 2' offences.

The Bill includes 'an offence constituted by conduct involving an act or acts of terrorism' as a new class 1 offence (**item 7**). As stated earlier, existing class 1 offences include murder, kidnapping and narcotics offences. The effect of **item 7** is that interception warrants can be sought and obtained 'in connection with investigation of terrorism offences, however described in relevant legislation'.[40] This statement, from the Explanatory Memorandum, reflects the fact that the phrase 'an act or acts of terrorism' is not defined in the Bill, a matter discussed in the Concluding Comments to this Digest.

The Bill nominates two additional class 2 offences: serious arson (**item 12**) and offences relating to child pornography (**item 13**). Although the specific types of conduct involving child pornography are defined in the Bill,[41] what constitutes 'serious' arson is not defined.[42] The other precondition of class 2 offences, namely, that the offence be punishable by imprisonment for life or a period of at least 7 years, will apply also to these new offences.

The purpose of these amendments is to ensure telecommunications interception is available as an investigative tool in relation to these offences. This is particularly seen as important in relation to conduct involving terrorist acts and child pornography offences, the latter because of offenders' increasing use of telecommunications services such as the Internet and email.[43]

Delayed access message services

Item 15 inserts **new subsections 6(3)-(5)**. These amendments indicate when 'delayed access message services' such as emails and voicemails will be regarded as communications 'passing over a telecommunications system' and thus subject to the provisions of the Principal Act, including the requirement to obtain an interception warrant to access those communications. If, for example, a person needs to access a telecommunications service eg by dialling a number in order to access their voicemail, then an interception warrant is needed to access the voicemail message. If the recipient of the message does not need to use a line to access their voicemail, email or other 'delayed access message service', then that communication will be called a 'stored communication' and the Principal Act is not applicable. The Explanatory Memorandum remarks that, in such a case, some other form of lawful authority would be required before a third party could access the message or the email.[44]

Certifying officers

The Bill extends the classes of officer at the NSW Crime Commission, the ICAC and the NSW Police Integrity Commission who are 'certifying officers'. As stated above, the powers of 'certifying officers' include certifying a true copy of an interception warrant that can be received as evidence in court proceedings.

At present:

- members of the Crime Commission are certifying officers. **Item 3** provides that, in addition to members of the Commission, persons occupying the position of senior executive officers of the Commission are 'certifying officers' when appropriately authorised.

- two people at the ICAC are 'certifying officers'—the Commissioner and Assistant Commissioner. **Item 4** will include, in addition, appropriately authorised persons occupying the position of senior executive officers of the ICAC.

- Commissioners of the Police Integrity Commission, Assistant Commissioners and appropriately authorised senior executive officers are 'certifying officers'. **Item 5** amends the relevant provision so that authorised persons acting as senior executive officers as well as authorised senior executive officers themselves are 'certifying officers'.

Purposes for which intercepted information can be used

As described above, the Principal Act prohibits the communication to another person of information lawfully gathered by a telecommunications intercept, and the giving of such information in evidence in legal proceedings. This general prohibition is subject to a large number of exceptions, some of which are listed above. For example, information may be

given in evidence in 'exempt proceedings'. Information may also be communicated to another person for a 'permitted purpose'.[45]

The Bill inserts some additional exceptions, two relating to the possible dismissal of police officers, one relating to the WA Anti-Corruption Commission, and one relating to the ICAC.

'Permitted purpose'

As previously mentioned, lawfully intercepted information may be communicated for a 'permitted purpose', including decisions relating to the engagement, retirement or termination of the employment of Australian Federal Police officers. However, in relation to State and Northern Territory police officers, currently a 'permitted purpose' only includes decisions relating to the appointment, re-appointment, term of appointment or retirement of an officer or member of staff of that police force. **Item 9** will amend this to include decisions relating to termination of appointment. This will bring the situation into line with that applicable to AFP officers.

Intercepted information will also be able to be communicated in relation to proceedings relating to the termination of the employment both of members of the Australian Federal Police and the police forces of a State or the Northern Territory (**item 18**). This would include proceedings such as claims for wrongful dismissal.

Item 10 inserts a new 'permitted purpose' for which intercepted information may be communicated, namely, investigations and reports by the WA Anti-Corruption Commission into allegations of corrupt conduct, criminal conduct, criminal involvement or serious improper conduct by a police officer or public officer. The purpose of this amendment is to allow communication of intercepted information relating to investigations into misconduct which may fall short of constituting a criminal offence.[46] It is broadly similar to the existing power of the NSW Police Integrity Commission.

'Exempt proceeding'

As explained above, lawfully intercepted information may be given in evidence in an 'exempt proceeding'. 'Exempt proceedings' currently include police disciplinary proceedings, and other proceedings relating to misbehaviour by Commonwealth or State officers. **Item 11** will add proceedings relating to a decision by the Commissioner of the Australian Federal Police or the police force of a State or the Northern Territory to terminate the employment of a police officer. This will permit lawfully intercepted information to be used in evidence in such proceedings.

Communications by the chief officer of an agency

Section 68 permits the chief officer of an agency to communicate information lawfully intercepted on a warrant obtained by that agency to other agencies in certain circumstances. Information may be communicated to the police where it relates to the

commission of an offence, or relates to acts which may give rise to police disciplinary proceedings. Information may also be communicated to various State investigatory authorities (the Royal Commission into the NSW Police Service, the NSW Police Integrity Commission, the Inspector of the Police Integrity Commission, and the WA Anti-Corruption Commission and the QCC) where it may give rise to investigations by those bodies. The 2002 Bill, unlike the 2001 Bill, adds to this list the communication of information to the ICAC where the information may result in an investigation by the ICAC (**item 44**).

In addition, the amendments will mean that the chief officer of an agency may communicate information to the relevant Australian Federal Police, State or Northern Territory Police Commissioner if the information may cause the relevant police commissioner to terminate the employment of the police officers to whom the information relates (**items 41 and 43**).

Clarification of warrants to enter premises

The Bill clarifies that warrants issued under section 48 authorising entry onto premises are warrants in their own right. A section 48 warrant to enter premises can only be issued in circumstances where a judge or AAT member would have power to issue a telecommunications service warrant, in respect of either a class 1 or class 2 offence. It cannot be issued for a named person. A number of items redraft existing provisions to make this distinction clear (**items 16, 24, 25, 27, 30, 32, 34, 45 and 46**).

As with telecommunications service warrants, the conditions in Division 3 of Part VI of the Principal Act must be complied with before a section 48 warrant is issued (**item 31**). Unlike other warrants, since 22 June 2000 a warrant authorising entry onto premises does not have to be executed by the Australian Federal Police. Some minor amendments are made to various provisions to reflect this (**items 21 and 35-37**). Similarly, an agency does not have to inform a telecommunications carrier of the issue of a section 48 warrant (**item 38**). This is because this requirement would not be relevant to a warrant to enter onto premises, only to the other types of warrant which authorise interference with telecommunications services.

Some minor amendments are also made to correct drafting errors introduced by the *Telecommunications (Interception) Legislation Amendment Act 2000* (**items 23, 29, 33 and 39**). These amendments are retrospective to 22 June 2000, the date on which the *Telecommunications (Interception) Legislation Amendment Act 2000* commenced.

Other amendments

Items 1 and 2 repeal references to Federal Court judges in the *Customs Act 1901* and replace them with references to a 'Judge of a court created by the Parliament.' These amendments will permit Federal Magistrates and Family Court judges, as well as Federal Court judges, to issue listening device warrants under the Customs Act. This brings the

Customs Act into line with the Principal Act. As with interception warrants, judges must consent to be nominated to issue listening device warrants.

Items 14 and 17 replace references to a Victorian statute which has been repealed (the *Crimes (Confiscation of Profits) Act 1986* (Vic)) with references to the current legislation (the *Confiscation Act 1997* (Vic)).

Items 19 and 20 make minor amendments to headings, which more accurately reflect the contents of Parts V and VI. These amendments do not affect the substance of the Principal Act.

Items 6, 8, 26, 28, 40 and 42 insert the connectors 'and' and 'or' as required.

Schedule 2—Amendment of the *Telecommunications (Interception) Act 1979* relating to new and defunct State bodies

A number of State investigatory bodies are referred to in the Principal Act. Some of these bodies have the power to conduct telecommunications intercepts under warrant, others are able to receive lawfully intercepted information from intercepting agencies if the information is relevant to their own investigations. Some of these State bodies are now defunct, and some have been reconstituted and renamed. Additionally, a new State investigatory body has been established. The amendments in **Schedule 2** flow from these events.

Amendments relating to the Criminal Justice Commission, the Queensland Crime Commission and the Crime and Misconduct Commission

The Crime and Misconduct Commission (CMC) was formed on 1 January 2002 with the merger of the Criminal Justice Commission (CJC) and the Queensland Crime Commission (QCC). The CJC was created under the *Criminal Justice Act 1989* (Qld) to monitor, review, coordinate and initiate reform of the administration of criminal justice in Queensland. The QCC was established by the *Crime Commission Act 1997* (Qld) to investigate major and organised crime and criminal paedophilia. Under the provisions of the *Crime and Misconduct Act 2001* (Qld), the CMC will work to:

- combat and reduce the incidence of major crime in Queensland
- improve the integrity of the Queensland public sector, and
- reduce the incidence of misconduct in the Queensland public sector.[47]

There are a number of references to the CJC and the QCC in the Principal Act. For instance, the CJC is an 'eligible authority' and its Commissioners are 'certifying officers' for the purposes of the Principal Act. References to the CJC, the QCC and their enabling legislation are removed by the amendments and replaced with references to the CMC and

its enabling statute (**items 1-5, 7-14, 16, 18, 19, 21-23, 26-29, 31, 35, 37, 39, 41-43 and 45**).

One effect of these amendments is to enable the CMC, like its predecessor agencies, to be given information lawfully obtained by intercepting agencies if that information relates to a matter that could result in an investigation by the CMC (**item 45**). The amendments also make the CMC, like the CJC and the QCC, an 'eligible authority' for the purposes of the Principal Act. However, unless a declaration by the Commonwealth Minister is in force, the CMC will not be able to conduct telecommunications intercepts itself. No declarations were in force for the CJC or the QCC.

Item 46 is a transitional amendment that provides that anything done by the CJC or the QCC under the Principal Act before the commencement of **Schedule 2** is deemed to have been done by the Crime and Misconduct Commission. The Explanatory Memorandum explains:

> The provision is necessary as the merger [between the CJC and QCC] took effect on 1 January 2002, and will have the effect of deeming acts done by the predecessor Commissions to be treated as though they had been done by the Crime and Misconduct Commission. The provision is necessary to ensure that intercepted information that was otherwise lawfully communicated to the predecessor Commissions is not rendered unlawful by the merger.[48]

Amendments relating to the Royal Commission into the New South Wales Police Service

On 13 May 1994, Supreme Court Justice James Wood was appointed to head the Royal Commission into the New South Wales Police Service (the Wood Royal Commission) and report into the nature and extent of police corruption, the efficacy of the Service's internal informers policy, the Service's promotion system, the activities of its Professional Responsibility and Internal Affairs Branches, its impartiality in investigating prosecutions, and other associated matters relating to criminal activity, neglect or violation of duty. The Wood Royal Commission was given the ability to obtain lawfully intercepted information obtained by intercepting agencies as a result of the passage of the *Royal Commission into the New South Wales Police Service (Access to Information) Act 1994*. The Wood Royal Commission was wound up in 1997.

As the Wood Royal Commission no longer exists, references to it are removed by amendments in **Schedule 2** (**items 6, 15, 20, 24, 30, 33, 34, 36, 38 and 44**).

Amendments relating to the Western Australian Royal Commission into Police Corruption

In December 2001, Western Australian Premier, Dr Geoff Gallop, announced that a Royal Commission into Police Corruption would be established. The Commission will inquire into and report on whether, since 1 January 1985, there has been corrupt or criminal conduct by Western Australian police. The Commission is due to report in August 2003.

The amendments in **Schedule 2** add the WA Royal Commission to the list of 'eligible authorities' in the Principal Act (**item 17**) and insert other references to the Commission in relation to 'prescribed investigation' (**item 25**) and 'relevant offence' (**item 31**). The amendments also enable the WA Royal Commission to obtain information lawfully collected by other intercepting agencies for the purposes of its investigations (**item 45**). Before the WA Royal Commission could intercept telecommunications itself, it would need to be the subject of a Ministerial declaration under the Principal Act. **Item 32** inserts a definition of the 'Royal Commission into Police Corruption' into the Principal Act.

Transitional amendments

Subitems 46(2) and (3) empower the Governor-General to make regulations dealing with any transitional matters that might arise from the enactment of **Schedule 2**. The Explanatory Memorandum states that the amendments effected by **item 46** are designed to address 'unforeseen issues arising out of the merger of the Queensland Crime Commission and Criminal Justice Commission'. Additionally, as stated above, they are designed to deal with any other matter arising from the enactment of **Schedule 2**.

Concluding Comments

In his Second Reading Speech for the Bill, the Attorney-General said:

> The bill includes conduct involving terrorist acts as offences in relation to which a telecommunications interception warrant may be sought.
>
> These provisions, and other measures taken by the government, are designed to bolster our armoury in the war against terrorism and deliver on our commitment to enhance our ability to meet the challenges of the new terrorist environment.
>
> The inclusion of terrorist offences as warrantable offences in their own right properly acknowledges the seriousness of all terrorist offences and will assist law enforcement agencies to avail themselves of this investigative tool in their investigations into such activity.[49]

The Bill does not refer to 'terrorist offences'. Instead, class 1 offences in the Principal Act will be defined to include 'an offence constituted by conduct involving an act or acts of terrorism'. The reason, according to the Explanatory Memorandum, is to 'enable intercepting agencies to seek interception warrants in connection with the investigation of terrorism offences, however described in relevant legislation'. It is arguably unclear exactly which offences in Commonwealth, State or Territory law might be encompassed by this definition and which, in consequence, might be subject to investigation via the use of an interception warrant.[50]

Endnotes

1 Simon Bronitt, 'Electronic surveillance, human rights and criminal justice,' *Australian Journal of Human Rights*, 3(2), 1997, pp. 183–207 at p. 188.

2 Section 7.

3 Section 7.

4 Section 6.

5 Section 5.

6 Sections 9 and 9A.

7 Sections 11A-11C.

8 Section 10.

9 Sections 45, 45A, 46, 46A.

10 Section 5.

11 Section 5D.

12 Sections 9, 9A, and 11A–11C.

13 Section 39. See the definition of 'agency' in section 5.

14 For the purposes of the Principal Act the expression 'State' includes the Northern Territory (section 5).

15 Sections 34 and 35. Section 35 sets out the prerequisites for a Ministerial declaration.

16 *Telecommunications (Interception) Act 1979. Report for the Year Ending 30 June 2000.* A declaration was made under section 34 in relation to the Anti-Corruption Commission of Western Australia on 24 September 2001.

17 Section 36.

18 Section 68.

19 Section 42.

20 Sections 45, 45A, 46, 46A and 48.

21 The exemption is contained in section 67.

22 Sections 63 and 77. The exemptions are contained in sections 63A, 74, 75, 75A, 76 and 76A.

23 Section 5B.

24 Section 5.

25 Section 5.

26 'Relevant proceeding' is defined in section 6L and includes a prosecution (or forfeiture proceedings or proceedings to recover a pecuniary penalty) for a prescribed offence; extradition proceedings relating to a prescribed offence; police disciplinary proceedings; and

proceedings relating to misbehaviour or improper conduct by a Commonwealth or State officer.

27 Section 66.

28 Section 68.

29 Section 70.

30 Section 68.

31 Section 68.

32 Sections 56 and 57.

33 Section 60.

34 Section 61A.

35 Section 61.

36 Introduced on 13 March 2002. The original Bill [the Security Legislation Amendment (Terrorism) Bill 2002], which was introduced on 12 March 2002, was withdrawn on 13 March 2002 and the [No.2] Bill was substituted. The reason was that the Office of Parliamentary Counsel had drawn the Government's attention to a discrepancy between the title of the original Bill and the title referred to in the notice of presentation given by the Attorney-General. This discrepancy meant that the Bill's introduction was inconsistent with House of Representatives' Standing Orders. The withdrawal and re-introduction were designed to address this problem. See Mr Peter Slipper MP, House of Representatives, *Hansard*, 13 March 2002, pp. 1138–9.

37 Introduced into the House of Representatives on 21 March 2002.

38 As stated above, the Anti-hoax Bill has received Royal Assent.

39 Attorney-General, *News Release*, 'National Move to Combat Terror', 7 April 2002. The Attorney's News Release can be found at: http://www.ag.gov.au/aghome/agnews/2002newsag/37_02.htm (accessed 15 April 2002).

40 Explanatory Memorandum, p. 4.

41 Specifically, the offences are the production, publication, possession, supply or sale of, or other dealing in, child pornography; and consenting to or procuring the employment of a child, or employing a child, in connection with child pornography.

42 Note that there are some other existing class 2 offences that are qualified by the word, 'serious', including 'serious fraud' and 'serious personal injury'.

43 The Hon. Daryl Williams, AM QC MP, Second Reading Speech on the Telecommunications Interception Legislation Amendment Bill 2002, House of Representatives, *Hansard*, 12 March 2002, p.977.

44 Explanatory Memorandum, p. 7.

45 Section 67 and section 5.

46 Explanatory Memorandum, p. 5.

47 http://www.cjc.qld.gov.au/INDEX.html (accessed 27 March 2002).

48 Explanatory Memorandum, p. 22.

49 House of Representatives, *Hansard*, 12 March 2002, p. 977.

50 In contrast to 'terrorism', other class 1 offences might be seen as more clearly defined. For example, the definition of a class 1 offence in section 5 of the Principal Act refers to:

- murder, or an offence of a kind equivalent to murder
- kidnapping, or an offence of a kind equivalent to kidnapping
- a narcotics offence
- offences constituted by acts such as aiding and abetting or conspiring to commit the primary offences listed above.

Further, an application for an interception warrant for a class 1 offence in contrast with those for class 2 offences, and presumably because of the very serious conduct encompassed by those offences, needs to satisfy fewer statutory criteria (compare, for instance, paragraph 45(e) in relation to a telecommunications service warrant for a class 1 offence with subsection 46(2) in relation to a telecommunications service warrant for a class 2 offence). In other words, does the wording in **item 7** enable an undefined class of offences to be the subject of an application for an interception warrant which is tested against less stringent criteria than those available for class 2 offences?