Parliament of Australia
Department of Parliamentary Services

Parliamentary Library
Information analysis and advice for the Parliament

BILLS DIGEST

5 May 2005, no. 147, 2004–05, ISSN 1328-8091

Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Bill 2005

Jennifer Norberry
Law and Bills Digest Section

Contents

Purpose 3
Background 3
Telecommunications (Interception) Act 1979 3
Types of interception warrant 4
Who issues interception warrants and for what purposes can they be obtained? 4
Who can apply for an interception warrant? 4
Criteria that must be satisfied before a national security or foreign intelligence warrant can be issued 5
Criteria that must be satisfied before a law enforcement warrant can be issued 5
When can information obtained by law enforcement warrants be used and by whom? 5
Reporting and ASIO warrants 6
Inspections and reporting in relation to law enforcement warrants 6
Report to Parliament on law enforcement warrants for the year 2003-04 7
Commonwealth Ombudsman's annual report for the year 2003-04 8
Named person warrants 8
The Sherman Report 9
Recommendation 1 9
Recommendation 2 10
Government response to recommendations 1 and 2 10
Recommendation 3 10

Government response to recommendation 3 10
Recommendation 5 10
Government response to recommendation 5 11
Recommendation 8 11
The Government response to recommendation 8 11
Main Provisions 11
Schedule 1—Amendment of the *Criminal Code Act 1995* 11
Schedule 2—Amendment of the *Telecommunications (Interception) Act 1979* 12
Part 1—Emergency services 12
Part 2—Interception by radiocommunications inspectors 14
Part 3—Ancillary offences 14
Part 4—Civil forfeiture proceedings and named person warrants 14
Civil forfeiture orders 14
Reporting by the Ombudsman 15
Statistics on named person warrants 16
Part 5—Employees of carriers 17
Concluding comments 17
Endnotes 18

Crimes Legislation Amendment (Telecommunications Interception and Other Measures) Bill 2005

Date Introduced: 16 March 2005

House: Senate

Portfolio: Attorney-General

Commencement: Various commencement dates, some of which are retrospective—see Main Provisions sections of this Digest

Purpose

The Bill has a variety of purposes. These are described in detail in the Main Provisions section of the Digest. However, in brief, the Bill amends both the *Criminal Code Act 1995* and the *Telecommunications (Interception) Act 1979* (the TI Act). The TI Act amendments include the Government's response to recommendations of the Sherman review of 'named person' interception warrants.

Background

The amendments in the Bill primarily affect the *Telecommunications (Interception) Act 1979* (the TI Act).

Telecommunications (Interception) Act 1979

The objectives of the TI Act include:

- protecting the privacy of those who use the Australian telecommunications system by making it an offence to intercept communications passing over a telecommunications system, other than as permitted by the Act
- prescribing how interceptions can lawfully occur and what can be done with the information obtained from lawful interceptions.[1]

The TI Act prohibits the interception of 'a communication passing over a telecommunications system' except in specified circumstances. These circumstances include operating or maintaining a telecommunications system and pursuant to a warrant. Further, because of the way that the expression 'interception of a communication' is defined it is not an offence to listen to or record calls to certain emergency service numbers or publicly listed ASIO numbers.

Interceptions conducted in breach of the TI Act attract criminal penalties and give rise to civil remedies.

Types of interception warrant

ASIO and certain law enforcement agencies may obtain warrants in relation to a *single*, identified telecommunications service ('telecommunications service warrants') or any telecommunications *services* that are used or likely to be used by a particular individual ('named person warrants'). Additionally, ASIO can obtain foreign communications warrants.

Who issues interception warrants and for what purposes can they be obtained?

Broadly speaking, warrants can be obtained for three purposes. The first is for national security. The second is for the collection of foreign intelligence. These warrants are issued by the Attorney-General and, in some circumstances, by the Director-General of Security. The third purpose is for law enforcement. Law enforcement warrants are issued by an 'eligible judge'[2] or a nominated member of the Administrative Appeals Tribunal (AAT).[3]

In general terms, warrants for national security purposes can be issued when the Attorney-General is satisfied that a person is engaged in activities prejudicial to security and the interception of telecommunications services used by that person will assist ASIO to obtain intelligence relevant to security.[4] Warrants for the collection of foreign intelligence authorise the interception of communications, including foreign communications, so that foreign intelligence relating to the Commonwealth's defence or international affairs can be collected by ASIO.

Law enforcement warrants can only be issued in order to investigate 'class 1' and 'class 2' offences. Class 1 offences include murder, kidnapping, narcotics offences, terrorism offences and aiding or conspiring to commit such offences. Class 2 offences include offences punishable for life or a period of at least 7 years where the offender's conduct involves death or serious personal injury, drug trafficking, serious fraud, bribery, dealing in child pornography, people smuggling, money laundering or cybercrime.

Who can apply for an interception warrant?

ASIO's Director-General of Security can apply for an interception warrant for national security or foreign intelligence purposes.

The following agencies can apply for and obtain interception warrants for law enforcement purposes:

- the Australian Federal Police (AFP)
- the Australian Crime Commission (ACC)
- an 'eligible authority' of a State or the Northern Territory in respect of which a Ministerial declaration is in force. As at 30 June 2004, declarations were in force for the Victoria Police, NSW Crime Commission, NSW Police, Independent Commissions

Against Corruption, South Australia Police, Western Australia Police Service, the Police Integrity Commission, Western Australian Anti-Corruption Commission, and the Western Australian Corruption and Crime Commission.[5]

Other agencies that are 'eligible authorities' under the TI 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. These agencies are the police services of the Northern Territory, Queensland and Tasmania, the Queensland Crime and Misconduct Commission, the Inspector of the Police Integrity Commission, the Royal Commission into the Western Australian Police Service, and the Parliamentary Inspector of the Western Australian Corruption and Crime Commission.

Criteria that must be satisfied before a national security or foreign intelligence warrant can be issued

The Director-General of Security can issue an interception warrant for national security purposes in an emergency in the circumstances set out in the TI Act. Otherwise, the Director-General must ask the Attorney-General for a national security warrant and accompany this request with prescribed information. For instance, in the case of a request for a telecommunications service warrant the request must include a description of the service, the number allotted to the service by a carrier and indicate why the Director-General considers the warrant should be issued.

The TI Act also sets out what must accompany an application for a warrant authorising the collection of foreign intelligence. Different criteria must be satisfied depending on whether this is a telecommunications service, named person or foreign communications warrant for the collection of foreign intelligence.

Criteria that must be satisfied before a law enforcement warrant can be issued

An application by a law enforcement agency for an interception warrant must be accompanied by an affidavit containing prescribed information. Further, before issuing an interception warrant the eligible judge or AAT member must be satisfied of the matters set out in the TI Act. There are differences in the matters that must be made out depending on whether the application is for a telecommunications service warrant or a named person warrant. Different criteria also apply depending on whether the offence being investigated is a class 1 or a class 2 offence. For instance, before issuing a named person warrant for a class 2 offence investigation, the judge or AAT member must consider the gravity of the offence and how much the privacy of any person would be interfered with as a result of the warrant application being granted.

When can information obtained by law enforcement warrants be used and by whom?

Subject to certain exemptions, information lawfully gathered by a telecommunications intercept cannot be communicated to another person or given in evidence in legal proceedings. Exceptions include providing that information as evidence in 'exempt

proceedings', such as prosecutions for 'prescribed offences', [6] proceedings for confiscation or forfeiture of property or police disciplinary proceedings. Other exceptions include disclosure for 'permitted purposes', such as investigations into 'prescribed offences' and decisions about whether to institute 'relevant proceedings'.[7]

Reporting and ASIO warrants

There are public reporting requirements for law enforcement warrants (see below) but no equivalent requirements for interception warrants issued to ASIO. However, ASIO is required to report to the Attorney-General and, in some circumstances, classified information is also provided to the Leader of the Opposition. If an emergency warrant is issued by the Director-General of ASIO a copy of the warrant must be provided to the Attorney-General together with an explanation of why the Attorney-General would have been justified in issuing the warrant and a statement that national security was likely to be seriously prejudiced.

Further, a report must be given to the Attorney-General within three months after a warrant has expired stating how the warrant has helped ASIO carry out its functions. Additional information must be provided in the case of a named person warrant.

As well as reporting requirements under the TI Act, the *Australian Security Intelligence Organisation Act 1979* is also relevant. It requires ASIO to give the Attorney-General an annual report on its activities. A copy of this report is also given to the Leader of the Opposition in the House of Representatives. Although this report details the number of TI warrants issued to ASIO, including the number of named person warrants, this information is classified and is deleted from the version of the annual report tabled in Parliament.[8]

Inspections and reporting in relation to law enforcement warrants

The TI Act contains many detailed record keeping and reporting requirements for law enforcement agencies. These serve as safeguard and accountability mechanisms. They include the following:

- the two Commonwealth agencies—the AFP and the ACC—must keep records about law enforcement interceptions and the use of intercepted information. Additionally, two registers must be kept by the AFP Commissioner. These are a General Register containing particulars of all law enforcement warrants. These particulars include the date of issue and period for which each warrant is in force, each serious offence the warrant related to, the telecommunications service intercepted, and the name of the subject. The Commissioner must also keep a Special Register containing similar details of expired warrants that do not result in a prosecution
- provision for agency reporting to the Attorney-General. The Attorney-General must be provided with the General and Special Registers on a quarterly basis and be given a copy of each warrant issued to an agency. Further, within three months of a warrant

ceasing to be in force, the Attorney must be given a written report about the use of information obtained by the interception

- the Commonwealth Ombudsman must conduct regular inspections of AFP and ACC records to ensure that interception activities are conducted in accordance with the statutory requirements. The Ombudsman must also report annually to the Attorney-General
- State legislation must contain parallel reporting requirements before the Attorney-General can make a declaration enabling the relevant 'eligible authority' to intercept telecommunications, and
- agencies must give the Attorney-General information required for inclusion in the annual report on the TI Act, which is tabled in Parliament.

Report to Parliament on law enforcement warrants for the year 2003-04

Division 2, Part IX of the TI Act lists the information that must be included in the annual report provided to Parliament on the TI Act. For instance, it must include the number of warrants applied for and issued, the number of arrests, prosecutions and convictions based on intercepted information and the use of judges and AAT members to issue warrants.

During 2003-04, 76% of law enforcement warrants were issued by AAT members, 6% by Family Court judges, 2% by Federal Court judges and 16% by Federal Magistrates.[9]

During 2003-04, 3028 warrants were issued to law enforcement agencies. This figure 'represents a decrease of approximately 1% on the total number of warrants issued during the previous reporting period'.[10] Thirty-one applications were refused or withdrawn, compared with nine refusals/withdrawals in the previous reporting year.

Although not a statutory requirement, the 2003-04 annual report also provides information about named person warrants. In the 2003-04 year, 429 named person warrants were issued and one application was refused/withdrawn. Twelve hundred and sixty-two services were intercepted under named person warrants. Fifty-one of those warrants intercepted one service each; 171 of those warrants intercepted between 2 and 5 services; 27 warrants intercepted between 6-10 services and 4 warrants intercepted more than 10 services.[11]

According to the annual report:

- 2035 arrests were obtained on the basis of information that was or included lawfully obtained information from intercepts. This represented an increase of 32% on the previous year's figures. There were 67 arrests for every 100 warrants issued, compared with 50 arrests for every 100 warrants in the previous year
- there were 2658 prosecutions in which information lawfully obtained from interceptions was given in evidence and 1824 convictions in which lawfully obtained information was given in evidence. The report records that this is a 27% increase in the number of prosecutions and a 48% increase in the number of convictions from the

previous year, amounting to 87 prosecutions and 60 convictions for every 100 warrants issued.

However, these figures do not reveal how many telecommunications services were intercepted to obtain the arrests and prosecutions or how the number of services intercepted has grown since the introduction of named person warrants.

Commonwealth Ombudsman's annual report for the year 2003-04

During the 2003-04 year, the Commonwealth Ombudsman conducted two inspections at the AFP and two at the ACC and reported on those inspections to the Attorney-General. The details of such reports are not made public. However, the Ombudsman's annual report contains a brief statement about its functions under the TI Act:

> The reports concluded that the agencies are generally complying with the requirements of the TI Act. However, there are also opportunities to improve the administrative and compliance systems for both agencies, especially in developing guidelines and training to assist staff in administering telecommunications interception warrants.[12]

Named person warrants

Several of the amendments proposed by the Bill are the Government's statutory response to the recommendations of the Sherman Report—the *Report of the Review of Named Person Warrants and Other Matters*.[13]

The origins of the Sherman Report can be traced to a recommendation made by the Senate Legal and Constitutional Legislation Committee when it inquired into the Telecommunications (Interception) Legislation Amendment Bill 1999. This Bill, which became the *Telecommunications (Interception) Legislation Amendment Act 2000* (the 2000 Act) contained a number of important amendments to the TI Act, particularly the addition of 'named person warrants'.

'Named person warrants' allow any telecommunications *services* used or likely to be used by a particular *individual* to be intercepted. Named person warrants are significantly more privacy intrusive than telecommunications warrants, which relate to a *single* telecommunications service. They have the potential to impact on greater numbers of innocent third parties who use the same telecommunications services as the subject of the warrant.

Prior to the introduction of named person warrants, warrants could only be issued for a particular telecommunications *service.* The TI Act dates from 1979 and, reflecting telecommunications services of the time, was premised on a new warrant being required for *each* telecommunications service accessed by a particular suspect. Named person warrants were introduced in response to technological developments which enable people to choose between and use a variety of services, such as multiple mobile phones combined with multiple SIM cards.[14] In these circumstances, requiring a separate

telecommunications service warrant to be obtained for each service used by a person was considered to be a counter-productive and unwieldy mechanism by law enforcement agencies and ASIO.

The Senate Committee concluded that the reporting mechanisms contained in TI Act and proposed in the 1999 Bill would play a crucial role in ensuring that named person warrants were not abused. It recommended that the Bill proceed.[15] However, it also recommended that the Bill 'provide for a review of its operations within three years of coming into effect', having regard to the need for the new warrant, the adequacy of safeguards and the adequacy of reporting mechanisms.[16]

The Government responded to the Senate Committee report by:

> … agree[ing] to a review of the operation of the bill as proposed by the committee. It will take place within three years of the bill coming into effect, and it will have regard to the three matters that have just been mentioned.[17]

A former head of the National Crime Authority, Tom Sherman AO, was asked by the Government to report on the need for named person warrants, the adequacy of safeguards governing their use, the adequacy of reporting mechanisms for monitoring the issuing and use of such warrants, and other matters.

The Sherman Report

The *Report of the Review of Named Person Warrants and Other Matters* was completed in June 2003. Mr Sherman concluded '… the regulatory regime generally contains adequate safeguards and reporting mechanisms. The regime has a strong compliance culture which is well audited by the inspecting authorities.'[18] Nevertheless, he recommended some 'relatively small changes …' Some of recommendations envisaged statutory changes and others were procedural or administrative in nature.

The Bill responds to three of Mr Sherman's recommendations: those relating to civil forfeiture orders, reports by the Commonwealth Ombudsman and statistical information for named person warrants. Details are provided in the Main Provisions section of this Digest. The remainder of Mr Sherman's recommendations and the Government's responses to them are as follows:

Recommendation 1

> That TI systems operating in each of the intercepting agencies and the major carriers be the subject of an independent vulnerability/risk assessment once every five years. The ICC [Interception Consultative Committee] should develop a program of assessments and monitor the implementation of the program.[19]

Recommendation 2

> That intercepting agencies develop consistent procedures for the authorisation of additional services to be intercepted under named person warrants and that inspecting authorities pay particular attention to this area. The procedures should include the keeping of records of the applications to extend services (including the grounds of the application), the decision on the application, and the notification to the carrier (referring to the original authorising warrant).[20]

Government response to recommendations 1 and 2

The Minister has said that recommendations 1 and 2 are being addressed by the ICC.[21] The ICC includes senior policy or managerial representatives of intercepting agencies and is chaired by the Agency Co-ordinator, a statutory position established under the *Telecommunications Act 1997*.[22]

Recommendation 3

> Wherever practicable persons making applications for law enforcement warrants should include a lawyer and the deponent to the supporting affidavit.[23]

Government response to recommendation 3

The Minister has said that the Government will accept recommendation 3.[24]

Recommendation 5

> ASIO should publish in the public version of its Annual Report the total number of TI warrants and named person warrants applied for, refused and issued in the relevant reporting year.[25]

Mr Sherman indicated that the Inspector-General of Intelligence and Security supports the publication of the total number of national security warrants obtained by ASIO. He pointed out that New Zealand and Canada both publish such statistics, while acknowledging that neither the United Kingdom nor the USA does so.

Mr Sherman also remarked:

> I believe that there should be a limited form of disclosure of the total number of warrants and named person warrants executed by ASIO, because I have difficulty in accepting that the mere publication of total numbers of warrants will provide any meaningful information to ASIO targets to enable them to take counter measures. The information is simply too general to achieve such a purpose.
>
> Further, the fact that ASIO conducts TI is publicly known … Finally, in this regard, I am influenced by the fact that it has never been suggested (nor am I aware of any evidence)

> that the publication of such statistics has enabled law enforcement targets to take countermeasures.[26]

Government response to recommendation 5

The Government rejected this recommendation. The Minister commented that a recent report by the Parliamentary Joint Committee on ASIO, ASIS and DSD did not recommend such a change.[27] The Government also takes the view that ASIO discharges its accountability responsibilities by classified reporting to the Government and the Opposition and that the Sherman Report raised no new substantive arguments for changing the present arrangements.[28]

Recommendation 8

Prior to 2000, the definition of 'restricted record' in the TI Act was:

> *restricted record* means a record obtained by means of an interception, whether or not in contravention of subsection 7(1), of a communication passing over a telecommunications system.

The 2000 amendments added the words, 'other than a copy', to the definition. As a result, copies of records are now exempt from the record keeping and destruction requirements of the TI Act.

Mr Sherman considered that 'at least the copies of recordings and transcripts or other direct records of intercepted communications should be controlled in the same manner as original recordings'.[29] He recommended that:

> The definition of restricted record which existed prior to the 2000 amendments to the Interception Act should be reinstated.[30]

The Government response to recommendation 8

The Government rejected this recommendation because 'recent developments in technology, particularly the advent of digital communications technology, mean that it may be impractical and inappropriate for the Interception Act to seek to regulate [copies]'.[31]

Main Provisions

Schedule 1—Amendment of the *Criminal Code Act 1995*

Part 10.6 was added to the Criminal Code by the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004*.[32] It contains new telecommunications offences. These offences include operating a device that hinders the normal operation of a 'carriage service',[33] modifying a 'telecommunications device

identifier',[34] and child pornography material and child abuse material offences. The Criminal Code provides 'law enforcement officers' who act in good faith in the course of their duties and whose conduct is reasonable in the circumstances of performing their duty with a defence to these and other offences.

At present, the expression 'law enforcement officer' is defined with reference to the AFP; State, Territory and foreign police forces; the Australian Crime Commission; the Office of Commonwealth Director of Public Prosecutions and similar offices established under State and Territory law.

Item 1 of **Schedule 1** expands the definition of 'law enforcement officer' to encompass officers of the New South Wales Crime Commission, the Independent Commission Against Corruption and the WA Corruption and Crime Commission; staff of the NSW Police Integrity Commission and employees of other agencies prescribed by regulation.

The reason for these additions to the definition of 'law enforcement officer' is that, like those who currently fall within its ambit, these officers may be able to intercept telecommunications or be required to access or transmit child pornography or child abuse material in the course of their duties.

Because they are legislative instruments, any regulations prescribing agency employees as 'law enforcement officers' must be tabled in Parliament and are subject to disallowance by either House.

The amendment effected by **item 1** will commence retrospectively—on 1 March 2005. This is the date that the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act (No. 2) 2004* commenced.

Schedule 2—Amendment of the *Telecommunications (Interception) Act 1979*

Part 1—Emergency services

As indicated earlier, subsection 7(1) of TI Act contains a general prohibition on the interception of 'communications passing over a telecommunications system'. Exceptions to the statutory regime are provided in various ways. For instance, some activities—like maintenance activities and interception under a warrant—are listed in section 7 as exceptions to the prohibition. Other activities are excluded from the ambit of the Act because they fall outside the definition 'interception of a communication passing over a telecommunications system' contained in section 6.

At present, subsections 6(2A) and (2B) of the TI Act provide that listening to or recording communications to prescribed emergency services *numbers* operated by the police, a fire service or an ambulance service does not constitute an interception for the purposes of the Act. These provisions were inserted into the TI Act by the *Telecommunications*

Interception Legislation Amendment Act 2002. **Item 1** of **Schedule 2** repeals subsections 6(2A) and (2B).

Items 3 and 4 insert **new subsections 7(2) and (3)** into the TI Act. The effect of these new subsections is that the interception of communications made to or from a declared emergency service *facility* will be exempted from the general prohibition on the interception of telecommunications contained in subsection 7(1) of the Act.

Apart from being moved from section 6 to section 7, the Bill effects other changes to provisions relating to emergency services. For instance:

- the exemption will apply to 'emergency service *facilities*' rather than 'emergency services *numbers*'. The numbers currently prescribed for the purposes of the Act are: 000, 106 and 112. However, the Minister's second reading speech points out that emergency services actually use 'hundreds, if not thousands, of numbers …'[35]
- the amendments will capture calls made *from* as well as calls made *to* emergency services. The existing provision only covers calls made *from* emergency service numbers
- as well as police, fire services and ambulance services, an 'emergency service facility' will include *services for despatching or referring matters to the police, fire services or ambulance services.* This addition is designed to capture outsourced services
- there is no requirement in the Bill for emergency service interceptions to occur lawfully in the course of a person's duties. In contrast, the current exemption in the TI Act applies to a person 'lawfully engaged in duties …'[36]
- 'emergency service facilities' will be declared by the Attorney-General's written instrument. Such instruments will not be legislative instruments for the purposes of the *Legislative Instruments Act 2003*. At present, 'emergency service numbers' are prescribed by regulation.[37] An important difference between an instrument that is not a legislative instrument and a regulation is that the former is not subject to parliamentary scrutiny. It need not be tabled in Parliament and is not subject to parliamentary disallowance. The Explanatory Memorandum explains that the reason a declaration is not a legislative instrument is:

  > … to ensure that the locations of emergency services facilities are not publicly available.
  >
  > … These facilities represent critical operational infrastructure which needs close protection as their loss would endanger the public for so long as these services were unavailable. There are few benefits in having the location of these facilities made public, and any that do exist are far outweighed by the potential risks.[38]

The amendments relating to emergency services commence on proclamation or six months after Royal Assent, whichever is earlier (**clause 2**). They do not operate retrospectively and thus might potentially expose some emergency service workers—such as workers who

recorded conversations on numbers other than 000, 106 and 112—to penalties under the TI Act.

Part 2—Interception by radiocommunications inspectors

The Explanatory Memorandum explains that where a radiocommunications network is connected to a telecommunications network, the TI Act applies to prohibit the interception of radiocommunications by the Australian Communications Authority where they interconnect with fixed line telecommunications. **Part 2** is designed to provide a limited exception to this prohibition—if the interception is incidental to a statutory spectrum management function.

How the provisions in **Part 2** commence depends on the commencement of section 6 of the *Australian Communications and Media Authority Act 2005*.[39]

Part 3—Ancillary offences

As stated above, the TI Act enables law enforcement interception warrants to be granted in relation to what are called 'class 1' and 'class 2' offences.

'Class 1' offences include murder, kidnapping, narcotics offences, terrorism offences and ancillary offences involving aiding or conspiring to commit such offences. **Item 8** means warrants will also be available to investigate the ancillary offence of being an accessory after the fact in relation to class 1 offences.

Part 4—Civil forfeiture proceedings and named person warrants

The amendments in **Part 4** relate to the Sherman Report.

Civil forfeiture orders

Mr Sherman recommended that the TI Act be amended so that 'civil forfeiture proceedings are included in the definition of exempt proceeding in section 5B of that Act.'[40] The purpose of the recommendation was to enable TI material originally obtained under a warrant issued for the investigation of a class 1 or class 2 offence to be used in civil based restraining order proceedings under proceeds of crime legislation.

TI material obtained under a warrant issued for the investigation of class 1 and class 2 offences can already be used in *conviction-based* restraining order proceedings. However, it cannot be used in civil forfeiture proceeding—that is, proceedings that are *not* conviction-based and where a civil standard of proof is used to determine the derivation of the proceeds of crime.[41]

Item 9 of Schedule 2 does two things:

- it implements Mr Sherman's recommendation through its amendment of section 6K of the TI Act
- it also removes the list of Commonwealth, State and Territory proceeds of crime legislation presently contained in paragraph 6K(c) of the TI Act and instead enables relevant Commonwealth, State and ACT laws to be prescribed instead by regulation. Regulations must be tabled in Parliament and may be disallowed by either House.

Item 9 commences on proclamation or six months after Royal Assent, whichever is earlier (**clause 2**).

Reporting by the Ombudsman

Mr Sherman's report makes the following comment:

> Perhaps the most important safeguard under the Interception Act is the inspection role carried out by the Commonwealth Ombudsman on the ACC and the AFP; by the State Ombudsman and the South Australian PCA on their respective State intercepting agencies; and by the IGIS on ASIO.[42]

Inspections are designed to ensure that intercepting agencies like the AFP and the ACC comply with their record keeping responsibilities under the TI Act. Mr Sherman recommended that:

> All inspecting authorities should include *in their annual reports to Parliament* a summary of the TI inspections conducted in the relevant year together with a summary of any deficiencies identified as well as any remedial action taken.[43]

The amendments do not adopt Mr Sherman's recommendation insofar as reporting the details to *Parliament*.[44] Instead, **item 10** amends section 84 of the Principal Act—the section that deals with the Ombudsman's annual report to the Attorney-General on the results of its inspections of Commonwealth agencies. It will require the Ombudsman to include in his or her annual report to the *Attorney*:

- a summary of inspections conducted during the year
- particulars of any deficiencies that 'impact on the integrity' of the interception regime, and
- particulars of remedial action (if any) taken or proposed to address the deficiencies.

There is no statutory requirement that either the Ombudsman or the Attorney convey this information to Parliament.

Statistics on named person warrants

At present, the TI Act does not require law enforcement agencies to report publicly the number of named person warrants issued annually or the number of telecommunications services intercepted under those warrants.[45]

Mr Sherman commented:

> When reporting related only to single service warrants there was a direct correlation between the number of warrants issued and the number of services intercepted. This is no longer the case. One named person warrant may result in the interception of a significant number of services. This means that the current statistical reporting provides no indication of the number of services being intercepted in the Australian community. Indeed the current statistics may be misleading in this regard.[46]

Mr Sherman recommended that the TI Act:

> … be amended to require each law enforcement intercepting agency to provide to the Minister statistics for each financial year on the
>
> number of named person warrants applied for, refused and issued;
>
> the number of named person warrants which involved the interception of services in the following ranges – one service, 2-5 services, 6-10 services and more than 10 services;
>
> the total number of services intercepted under named person warrants;
>
> and that those statistics be set out in the Annual Report on the Interception Act tabled in Parliament.

Items 12 and **14** amend section 100 of the TI Act—the section dealing with the statistics that must be included in the Attorney-General's annual report to Parliament. They will require the report to include aggregate statistics about:

- the number of applications for named person warrants, statistics about telephone applications, renewal applications and applications that involved entry onto premises and how many named person warrants were issued subject to conditions
- how many named person warrants involved the interception of a single telecommunications service, how many involved the interception of between 2-5 services; 6-10 services and more than 10 services, and
- the total number of telecommunications services intercepted by way of named person warrants.

These figures will also be broken down by each Commonwealth and State agency.

These items commence on Royal Assent (**clause 2**).

Part 5—Employees of carriers

Item 15 defines 'an employee of a carrier', an expression which appears in subsection 5(4) of the TI Act, to include a person 'who is engaged by the carrier or whose services are made available to the carrier'. This would include contractors.

The expression, 'an employee of a carrier', is an important one and appears in a number provisions in the TI Act. For instance, interception warrants do not authorise the interception of communications passing over a telecommunications system operated by a carrier unless the interception occurs as the result of action taken by an employee of the carrier.[47]

This amendment commences on 1 June 1980—the date the TI Act commenced.

Concluding comments

Parliament may wish to consider the following matters during its deliberations on the Bill:

- whether the TI Act or the ASIO Act should be amended to require the public version of ASIO's annual report to contain the total number of TI warrants and named person warrants applied for, refused and issued during each reporting year. Such an amendment would constitute a statutory implementation of recommendation 5 of the Sherman report and, to borrow Mr Sherman's words, could be seen as a 'modest step towards greater disclosure and accountability'[48]
- whether there should be legislative amendment to implement recommendation 6 of the Sherman report and require the Commonwealth Ombudsman's annual report to Parliament to contain details of inspections of the AFP and ACC conducted during the year, particulars of deficiencies revealed and remedial action taken or proposed. As indicated earlier in this Digest, the proposed amendments require the Ombudsman's report to the Minister to contain these details but are silent about reporting to Parliament
- whether retrospective protection should be given to workers in emergency facilities who may have listened to or recorded emergency calls on numbers other than 000, 106 and 112 (see the discussion of **items 3 and 4** in the Main Provisions section of this Digest).

Parliament may also wish to keep a watching brief on the matters raised in recommendation 2 of the Sherman report—relating to the development of consistent procedures for the authorisation of additional services to be intercepted under named person warrants. Mr Sherman also recommended that inspecting authorities pay particular attention to this area. The Government has said that recommendation 2 is being addressed by the Interception Consultative Committee. Mr Sherman did not recommend that recommendation 2 should be the subject of legislative amendment but added:

> … it may it necessary in relation to record keeping in order to give the inspecting authorities a clearer role in this area. Another course might be to consider the need for legislation in the light of experience, particularly if obstacles emerge to Ombudsmen carrying out this role.[49]

Endnotes

1 For an overview of the TI Act see *Telecommunications (Interception) Act 1979. Report for the year ending 30 June 2004*.

At http://www.ag.gov.au/agd/WWW/agdhome.nsf/Page/RWP3BD452E345D42468CA256FD5001672B8

2 An 'eligible judge' is a federal judge who has consented in writing to be nominated for the purposes of the Act and who has been declared by the Attorney-General to be an eligible judge.

3 Nominated AAT members are Deputy Presidents and certain senior members and members of the AAT.

4 There are some differences in the requirements for telecommunications service and named person warrants and additional requirements for named person warrants.

5 TI Act, Annual Report, op. cit.

6 'Prescribed offences' include class 1 and class 2 offences, telecommunications offences under Part 10.6 of the Criminal Code and offences punishable by at least three years imprisonment.

7 For example, prosecutions for 'prescribed offences'.

8 Tom Sherman AO, *Telecommunications (Interception) Act 1979. Report of Review of Named Person Warrants and Other Matters*, June 2003, pp. 32 & 35.

9 TI Act, Annual Report, op. cit.

10 ibid, p. 17.

11 ibid, op. cit, pp. 45-8.

12 Commonwealth Ombudsman, *Annual Report 2003-2004*, p. 62.

13 At http://www.ag.gov.au/agd/WWW/agdHome.nsf/Page/Publications_Publications_2003_Report_of_Review_of_Named_Person_Warrants_and_Other_Matters

14 Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Telecommunications (Interception) Legislation Amendment Bill 1999*, May 2000.

15 ibid. p. vii.

16 ibid.

17 Senator Amanda Vanstone, Senate, *Parliamentary Debates*, 7 June 2000, p. 14772.

18 Sherman, op. cit, p. vii.

19 ibid, p. 23.

20 ibid, p. 29.

21 Minister for Justice and Customs, Second reading speech, Senate, *Parliamentary Debates*, 16 March 2005, p. 2.

22 See Sherman, op. cit.

23 ibid, p. 31.

24 Minister for Justice and Customs, Second reading speech, Senate, *Parliamentary Debates*, 16 March 2005, p. 2.

25 Sherman, op. cit, p. 38.

26 ibid, p. 37.

27 As Mr Sherman points out, the Committee did not come to a conclusion but 'it seems implicit by its omission to do so that it accepted ASIO's position [ie against publication] on the matter'. Parliamentary Joint Committee on ASIO, ASIS and DSD, *A Watching Brief: the Nature, Scope and Appropriateness of ASIO'S Public Reporting Activities*, September 2000, p. 37:

http://www.aph.gov.au/house/committee/pjcaad/asio/pubrepreport.htm

28 Minister for Justice and Customs, Second reading speech, Senate, *Parliamentary Debates*, 16 March 2005, p. 3.

29 Sherman, op. cit, p. 48.

30 ibid.

31 Minister for Justice and Customs, Second reading speech, Senate, *Parliamentary Debates*, 16 March 2005, p. 2. The Minister's second reading speech refers to "original" records. This is an error.

32 The 2004 Act also repealed the old telecommunications offences previously contained in the *Crimes Act 1914*.

33 Including the Internet and emails.

34 This identifier enables carriers to correctly identify and block lost or stolen mobile phones. Offences relating to telecommunications device identifiers are aimed at those who attempt to evade mobile phone blocks by altering the identifier.

35 Minister for Justice and Customs, Second reading speech, Senate, *Parliamentary Debates*, 16 March 2005, p. 2.

36 Subsection 6(2B), TI Act.

37 Telecommunications (Interception) Regulations 1987.

38 Explanatory Memorandum, p. 6.

39 Section 6 is the provision that establishes the Australian Communications and Media Authority. It will commence on proclamation or on 1 July 2005, whichever occurs earlier.

40 Sherman, op. cit, p. 46.

41 ibid.

42 ibid, p. 23.

43 ibid, p. 39. Emphasis added.

44 The Explanatory Memorandum states that the amendments will require '… the Ombudsman … to include in its *annual report to Parliament* a summary of the telecommunications interception inspections conducted in the relevant year together with a summary of any deficiencies identified and any remedial action taken', p. 7. This is an error.

45 Sherman, op. cit.

46 ibid, p. 34.

47 Explanatory Memorandum, p. 9.

48 Sherman, op. cit, p. 38.

49 ibid, p. 29.

Members, Senators and Parliamentary staff can obtain further information from the Information and Research Services on (02) 6277 2476.