Parliament of Australia
Department of Parliamentary Services

Parliamentary Library
Information analysis and advice for the Parliament

BILLS DIGEST

28 February 2006, no. 102, 2005–06, ISSN 1328-8091

Telecommunications (Interception) Amendment Bill 2006

Sue Harris Rimmer
Law and Bills Digest Section

Contents

Telecommunications (Interception) Amendment Bill 2006

Date Introduced: 16 February 2006

House: House of Representatives

Portfolio: Attorney-General

Commencement: Schedule 1 (Stored communications), Schedule 2 (B-party interception) and Schedule 3 (Equipment-based interception) will commence on the day after the Bill receives Royal Assent. Schedule 4 (Class 1 and class 2 offences) commence on 1 July 2006. Schedule 5 (Transfer of functions) will commence on a day to be fixed by Proclamation. Schedule 6 (Other amendments) will commence on the day on which this Act receives Royal Assent or as otherwise specified by this Bill.

Purpose

The purpose of this Bill is to amend the *Telecommunications (Interception) Act 1979* (the Act) to implement certain recommendations of the Blunn Report on the review of the regulation of access to communications under the Act.

Background

Basis of policy commitment

In implementing recommendations of the Blunn Report, the *Explanatory Memorandum* states that this Bill will amend the Act to:

- insert a warrant regime for access to stored communications held by a telecommunications carrier
- enable interception of communications of a person known to communicate with the person of interest
- enable interception of telecommunications services on the basis of the use of a telecommunications device
- remove the distinction between class 1 and class 2 offences for which telecommunications interception powers are available to law enforcement agencies, and
- remove the Telecommunications Interception Remote Authority Connection function currently exercised by the Australian Federal Police and transfer the associated warrant register function to the Department administering the legislation.

This Bill will also amend the Act to:

- remove the exception to the definition of interception in subsection 6(2) of the Act
- clarify that employees of a carrier exercise authority under a telecommunications interception warrant when assisting law enforcement agencies in the execution of interception
- include an additional permitted purpose for use and communication of lawfully obtained information in relation to the Victorian Office of Police Integrity, and
- update applicable references to money laundering offences in New South Wales.[1]

Stored communications

The primary object of the Act is to protect the privacy of personal communications by generally prohibiting interception of those communications, subject to limited exceptions in which privacy is outweighed by other considerations. Thus, until this bill, interception has been prohibited, except for specific enumerated exceptions. Indeed, the Blunn report found that although phone tapping was essential for fighting crime and protecting national security, there should be tighter laws to protect privacy.

The *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* introduced into the Act the concept of a 'stored communication' (paragraph 7(3A)) and provided that a stored communication could be intercepted without the need for a telecommunications interception warrant (paragraph 7(2)(ad)).[2] Access to such communications could therefore be obtained by other lawful means, such as by a normal search warrant.

A 'stored communication' broadly defined includes electronic messages located on a computer, internet server or other equipment, whether read or unread, such as emails, text messages and voicemail. Subsection 7(1) of the Act prohibits interception of communications 'passing over' a telecommunications system. The confusion that arose was that in certain situations emails, text messages, voice mail etc can be deemed to be no longer 'passing over' any such system.

The Attorney-General Philip Ruddock was quoted in the media stated that the Bill was necessary because terrorist suspects were going to 'extraordinary lengths' to avoid detection:

> Evasive techniques included daily swapping of mobile phone SIM cards; storing draft emails in accounts, but not transmitting them; and using the phones of other people.
>
> …I know that because I see a lot of the material that is yielded, where people are talking in veiled language, using all sorts of techniques. We have to keep moving as well and keeping up to date.[3]

The stored communications amendments in 2004 were intended as an interim measure pending a review by Mr Anthony S. Blunn AO of the regulation of access to communications in Australia. The amendments were originally subject to a 12-month sunset clause meaning that the provisions were to cease operation on 14 December 2005. The *Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005* extended the sunset date until 14 June 2006 to provide sufficient time to consider the recommendations of the Blunn review. The *Report of the Review of the Regulation of Access to Communications* ('the Blunn Report')[4] was presented to Parliament on 14 September 2005 when the *Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Act 2005* was introduced.

See also the report on the May 2004 Bill by the Senate Legal and Constitutional Committee.

The Blunn Report recommended that:

- the distinction between real time access i.e. interception, and access to stored data be maintained
- access to stored communications continue to be authorised by search warrant but those warrants be required to meet minimum prescribed standards, and
- in the context of accessing stored communications any specific reference to Voice over Internet Protocol (VoIP) is unnecessary and should be removed.

For further detail see Bills Digest no. 53 2005–06, and Bills Digest No. 153 2003-2004. Bills Digest 111 2003-2004 sets out the differences between an interception warrant and an ordinary search warrant, and provides a historical overview of telecommunications interception in Australia.

This Bill will generally prohibit access to stored communications in the same manner as telecommunication interceptions are currently prohibited (see **Schedule 1, new section 108**), with some key differences (outlined in **new Part 3.3**). New Chapter 3 contains the new stored communications provisions in seven Parts:

- prohibition on access to stored communications
- access by Australian Security Intelligence Organisation (ASIO) to stored communications
- access by enforcement agencies to stored communications
- dealing with accessed information
- keeping and inspection of access records
- reports about access to stored communications, and
- civil remedies.

B-Party interceptions

The Blunn Report defines B-Party intercepts as occurring

> where there is evidence that a person, other than a person suspected of involvement in the prescribed crime, the B-Party, is using a telecommunications service for communications which are believed to be relevant to the investigation. The B-Party may simply be a conduit for a relevant communication and may not even be aware of the use being made of them.[5]

B-party interceptions are not new. They are currently provided for under section 46(1) of the existing Act but Blunn notes that the section has not been utilised by the relevant agencies as the provisions were seen as open to several interpretations. As it is an intrusive power affecting non-suspects, the legislation should therefore be construed strictly.

The Blunn review recommended the legal status of B-Party interceptions be clarified 'to make it clear that B-Party services may be intercepted in limited and controlled circumstances'.[6]

The only direct consideration of this aspect of section 46 by a court since its introduction was in the case of *Flanagan v AFP* (1996) 60 FCR 149. One issue in question in the *Flanagan* case was where the subscriber of a telephone service intercepted was not the particular person being investigated in respect of the offence, or as the judgment itself states at section 6.5, 'whether the scope of the TI warrant exceeded what the legislation permits such a warrant to authorise' (at pages 201–2). The target of the investigation was Mr Flanagan, but the subscriber to the telephone service that was intercepted was his wife, Mrs Flanagan.

The applicants, the Flanagans, argued that the TI warrant authorised interceptions beyond those contemplated by the scheme of the TI Act because they were not limited to communications made to or from the relevant service which would be likely to assist in the investigation of the specified criminal offences. They further argued that, since the subscriber for the service in question was Mrs Flanagan, it was highly probable that at least some communications to and from the service would have nothing whatever to do with Flanagan or Bruno Grollo, being the 'particular person' whom the eligible Judge was satisfied was using or likely to use the service. Those extraneous communications would be unlikely to assist in the investigation of any relevant class 2 offence and, therefore, did not come within the ambit permitted by the phrase 'such communications' in s 46(1)(e).

The Federal Court rejected that argument as a matter of statutory interpretation and practicality and found that *all* communications made to or from the service could be monitored and the warrant was valid.

> Until a communication to or from a service has been intercepted and recorded, it is impossible to know whether it would be likely to assist in an investigation, or even to identify the parties to the communication. If warrants were confined to authorising the

> interception of communications to which the particular person could be identified at the outset as a party, they would lose much of their efficacy. This cannot have been intended.
>
> …There is no requirement that the prescribed offence be one in which the particular person contemplated by s 46(1) is involved.[7]

Blunn states in relation to this case:

> … although the Federal Court in *John Flanagan v The Commissioner of the Australian Federal Police* has upheld the validity of a B-Party warrant it did not provide any useful analysis of the rationale.[8]

Blunn is not expansive in his explanation of the rationale for B-Party warrants either, other than his view that such intercepts are useful in certain circumstances.[9]

Nevertheless, as noted, the agencies have not sought to act under this power as a matter of caution. The amendments made by this Bill seem designed to cover both possible interpretations of the term 'person involved' to remove all possible doubt and therefore enable the agencies to seek B-Party warrants. There may be limited scenarios where the communications of a person targeted by a B-Party warrant could not already be monitored under a named person warrant.

The B-Party warrant will only be available for investigations of serious offences punishable by a maximum period of at least seven years imprisonment, and as a last resort.

Equipment-based interception

As per the discussion of B-Party warrants above, the Bill seeks to expand the possibilities of interception to cover all evasive techniques criminals may take using new technologies. The purpose of Schedule 3 is to amend the named person telecommunications interception warrant provisions to enable interception agencies to intercept communications to and from identified devices such as mobile handsets and computer terminals.

An issuing authority must not authorise interception on the basis of the telecommunications device unless satisfied that the applicant agency has 'no practicable methods of identifying the telecommunications services used or likely to be used by the person of interest, or that interception of those services would not be possible' (**Schedule 3, item 8**).

The Explanatory Memorandum notes:

> The latter situation covers instances in which agencies may be able to identify all services, but it is impractical to intercept each service. For example, a person of interest may transfer hundreds of different Subscriber Identity Module (SIM) cards through a mobile handset in quick succession. Interception of each

> telecommunications service (currently identified by reference to the SIM card) is extremely impractical to achieve before the person of interest changes the SIM card being used.[10]

Position of significant interest groups/press commentary

Most press and interest group commentary has been in relation to the issue of B-Party warrants. Mr Cameron Murphy, Chair of the NSW Council for Civil Liberties has argued that:

> This is the first time ever in Australia's history that we see the police being given the power to tap the phones of people who are not suspects, who are innocent people and just people who happen to be in contact with someone, likely to be in contact with someone who's a criminal. And it massively expands police surveillance and it's directly targeted against innocent people who are doing nothing wrong.[11]

In another interview, Mr Murphy told 2CC radio there was no demonstrated need for the laws:

> I can't think of a real, practical situation where these powers would be needed. The way the law stands at the moment is that the police and many other agencies in Australia can obtain a warrant to tap a particular phone line. They've already got the power to do that. They can also apply to obtain a warrant to tap on the basis of a named person, so they can tap any phone that that named person is likely to use. So it can cover a range of phones, not just the one line—particular line.[12]

The Section President of International Commission of Jurists Australia, the Hon Mr John Dowd also stated in the press that the B-party intercepts were 'an unwarranted extension of police and ASIO powers for which no justification has been given'.[13]

The NSW Council for Civil Liberties main concern, as expressed in the media, is the right to privacy of non-suspects:

> … Now, on the phone, people make private conversations. They might be talking to a loved one, they might be discussing a medical condition with a doctor. They're incredibly personal and private things…

It may be an evolving question where the balance lies in privacy issues where crime and national security are involved in Australia. In introducing the Bill to the House, Attorney-General The Hon. Philip Ruddock addressed the question of whether Australian communications were intercepted more than American communications in the following manner:

> I note that critics of Australia's interception regime have again advanced old arguments that Australian agencies intercept communications at many times the rate of United States agencies and others.

> As I have pointed out on a number of previous occasions, it is simply not true to complain that Australians are intercepted more than Americans. Direct comparisons between Australian and US statistics are misleading because legislative controls on interception differ widely between jurisdictions.
>
> Statistics published in the United States do not include interceptions considered by the investigators to be too sensitive to report. Investigators in Australian law enforcement agencies do not have this discretion and therefore all interceptions must be reported.
>
> United States law allows one warrant to authorise the interception of services used by many people, for instance where it becomes possible to identify criminal associates of the original suspect.
>
> This results in fewer statistical returns than under Australian law, which allows a warrant to authorise the interception of a single telecommunications service or the services of one named person only.
>
> Comparisons of the type made both recently and in the past are therefore misleading and unfairly impugn our law enforcement agencies. The use of interception is subject to strict controls and it is a tool to be employed only in the investigation of the most serious offences.

The Attorney-General was presumably referring to media statements made by the NSW Council of Civil Liberties Chair Mr Cameron Murphy in January and February of this year. The statements were based on a comparison of a report by the Attorney-General's Department, *Telecommunications (Interception) Act 1979: Report for the year ending 30 June 2004,* released in March 2005, and a report by the Administrative Office of the US Courts, *2004 Wiretap Report*, from April 2005.

The Council stated:

> Recently released figures show that telephone wiretapping by government agencies in Australia (including the police) continues to grow. Not only does Australia issue 75% more telecommunications interception warrants than the US, but ***per capita*** Australia issues 26 times more warrants than the US. In Australia non-judges issue 76% of all warrants, whereas in the US only judges can issue warrants.
>
> In the twelve months 2003/2004 there were 3028 warrants issued in Australia. In the twelve months of 2004, US courts issued 1710 warrants. Adjusting for population, Australia intercepts telephone communications 26 times more *per capita* than the United States.
>
> Worryingly, the numbers are way up on figures only two years ago. In 2001 there were more than 2150 warrants issued in Australia, compared with only 1490 warrants issued in the United States of America. Australia intercepted telephone communications 20 times more *per capita* than the United States.

The Council blames the increase in phone-tapping on AAT members acting as issuing authorities:

> In Australia it is illegal to intercept telecommunications without a warrant. However, these warrants can be issued by people other than judges. Members of the Administrative Appeals Tribunal ('AAT') who have been lawyers for more than five years can be nominated (by the government) to issue warrants. In the reporting year 2003/2004, the vast majority of warrants (76%) were not issued by judges, but by members of the AAT.
>
> AAT members do not have tenure, are appointed by the government and work on contract. This means that AAT members are more likely to do the government's bidding than a judge, which explains why most warrants are issued by non-judges.[14]

The Australian figures include interceptions by the National Crime Authority, the Australian Federal Police and state policing agencies, but exclude ASIO. The US figure includes federal and state law enforcement agencies and some FBI taps. Only judges can approve phone taps in the US but there has been recent controversy over the revelation by President Bush that he ordered the National Security Agency to monitor communications in secret without warrants since 2001 in a 'terrorist surveillance program'.

Given the nature of the reporting and the lack of comprehensive statistics on phone tapping from either the US or Australia, comparisons may be difficult to make. The premise of the question may be wrong in any event – should the yardstick by which the private communications of Australian citizens are monitored be set by another country?

ALP/Australian Democrat/Greens policy position

The *Sydney Morning Herald* reported disquiet over the Schedule 2 B-Party amendments by five backbench members of the Coalition, naming three, the National Party's Paul Neville, the Sydney Liberal MP Bruce Baird and the Victorian Liberal Petro Georgiou.[15]

In a Joint Statement by Arch Bevis MP (Shadow Minister for Homeland Security), Senator Joe Ludwig (Shadow Minister for Justice and Customs), and Nicola Roxon MP, Shadow Attorney-General on 15 February 2006, Labor 'cautiously' welcomed the introduction of the Bill because:

> These changes will bring the Act up to date and put the state and federal law enforcement agencies on a more even footing with criminals and terrorists.[16]

The statement confirmed that Labor will seek to refer the Bill to the Senate Legal and Constitutional Committee and pay particular attention to B-party communications, but felt it was clear that the current legislation had been overtaken by developments in technology and was in need of review.

Senator Natasha Stott Despoja, Australian Democrats spokesperson for the Attorney General's portfolio stated that the Australian Democrats will challenge the Bill because 'it represents yet another unjustified intrusion on the private lives of Australians'.

> The Blunn Review did not argue the case sufficiently to justify such invasive laws on stored communications. The pretence of 'modernising surveillance' is a weak argument.
>
> The tests and oversight that the Attorney-General is promising are a completely inadequate defence for these disturbing new laws.[17]

Greens Leader Bob Brown issued a press release on 15 February 2006 stating that allowing police and spy agencies to monitor the phone calls, emails and text messages of people not suspected of a crime represents a dangerous incursion on civil liberties:

> The Howard government wants to give police the power to tap the phones of innocent people – people the police don't even suspect of a crime. Surely Australians who are suspected of no crime are entitled to their privacy...This is a new low in the preservation of our civil liberties.[18]

Main Provisions

Schedule 1 – Stored communications

Definitions

Part 1, item 1 inserts a definition of *stored communication* into existing subsection 5(1) of the Act. A stored communication is defined to mean a communication with four specific elements:

- the communication must have passed over a telecommunications system (therefore not stored draft emails)
- the communication must not be passing over that or any other telecommunications system (clarified in new **section 5F**)
- the communication must be held on equipment operated by the telecommunications carrier at its premises. The regime does not affect existing lawful access to communications stored on a person's telecommunications device such as a mobile phone handset, which remain subject to general lawful access including access by consent, or under a general search warrant, or a notice to produce, and
- the communication must be accessible to the intended recipient of the communication (defined further in new **section 5G** ('intended recipient') and new **section 5H** ('able to access')).

Item 2 inserts four new definitional sections into the Act. New **section 5E** defines *serious contravention*, which must be, or have been, committed, or be reasonably suspected of being committed for an enforcement agency to be able to obtain a stored communications warrant (new **subsection 5E(2)**).

New **subsection 5E(1)** defines serious contravention to be a contravention against a law of the Commonwealth, a State or a Territory that is:

- a 'serious offence' (the existing threshold for obtaining a telecommunications interception warrant, as defined by section 5D)
- an offence punishable by imprisonment for a period, or a maximum period, of at least three years, or the equivalent pecuniary penalty (which is at least 180 penalty units for individuals or at least 900 penalty units for corporations), or
- a breach of a civil penalty provision that would render the person committing the contravention liable to a fine of at least 180 penalty units ($19,800) (or at least 900 units ($99,000) if the person is a corporation).

New **section 5F** defines the concept of *passing over* a telecommunications system. It clarifies that a communication that is passing over a telecommunications system continues to do so until it can be accessed by the intended recipient of the communication.

New section 5G defines *intended recipient* as follows:

- where the communication is addressed to a person who is an individual, the intended recipient is that individual. This definition applies whether the individual is acting in his or her own capacity or as the employee or agent of another
- where the communication is addressed to a person who is not an individual such as a corporation, partnership, association or other group of persons, the intended recipient is any person within it who is able to access communications sent via that address
- where the communication is not addressed to a person but is sent to a generic address (such as an email address), the intended recipient is any person, or any employee or agent of the person, who has control over the telecommunications service to which the communication was sent.

New subsection 5H(1) provides that a communication is accessible to the intended recipient when it has been received by or has been delivered to the telecommunications service of the intended recipient, or is under the control of the intended recipient. **New subsection 5H(2)** ensures that new subsection (1) is not a prescriptive definition, and therefore does not limit the circumstances in which a communication is accessible to the intended recipient. The Explanatory Memorandum notes that:

> This definition is intended to be read broadly, to ensure that a communication is a stored communication even if the intended recipient has not obtained the content of the communication or is not even aware that the communication exists.

> 'Accessible' simply means that the communication is available to the intended recipient via their telecommunications device. It does not require that the intended recipient has read or listened to the communication, nor does it require the intended recipient to be aware of its existence. For example, an e-mail that is delivered to the inbox of an intended recipient is accessible even if the person is unaware of its presence or indeed not physically able to access the communication. [19]

This raises the question of the 'undeliverable' email. Presumably it will be able to be accessed under the new stored communication warrant.

Item 3 inserts **new section 6AA** into the Act, which defines the concept of *accessing* a stored communication to mean listening to, reading or recording a stored communication, by means of equipment operated by a carrier, without the knowledge of the intended recipient. The Explanatory Memorandum notes:

> The reference to the knowledge of the intended recipient is designed to protect the privacy of the communication before such time as the communication becomes accessible to the intended recipient. The requirement for knowledge also preserves the ability of law enforcement agencies to access stored communications held by a carrier where they do so with the knowledge of the intended recipient. For example, an enforcement agency may use its existing notice to produce at the carrier where they have notified the intended recipient that they intend to access the communications in this manner. This distinction means that enforcement agencies are regulated by the stored communications regime only when they are acting covertly in the access to these communications. When acting overtly, existing access and compulsion powers of the enforcement agencies remain applicable.[20]

The reference to 'by means of equipment operated by a carrier' reinforces the fact that the prohibition on accessing stored communications only relates to accessing these communications via the carrier.

In all other aspects, this definition is based on the definition of intercepting a communication in section 6 of the Act.

Item 4 inserts a **new section 6DB** into the Act which provides that the Minister responsible for the administration of the Act can, by writing, appoint as an issuing authority a judge of the federal court, including a judge of the Federal Court of Australia, Family Court of Australia or a Federal Magistrate, or a magistrate where those persons have consented in writing to be appointed as an issuing authority.

The amendment will also allow the Minister to appoint a person who holds an appointment to the Administrative Appeals Tribunal as Deputy President, full-time senior member, part-time senior member or member (including a part-time or full-time member), who is enrolled, and has been enrolled for at least 5 years, as a legal practitioner of a federal court or of the Supreme Court of a State or Territory. The appointment of AAT members as issuing authorities rather than judges has been the subject of strong criticism as noted below in the Concluding Comments to this Digest, and above at pages 7-9.

The addition of Commonwealth judicial officers as possible issuing authorities may raise Constitutional issues, as has been canvassed in the context of Division III of the *ASIO Act* and the *Anti-Terrorism (No. 2) Act 2005*. In summary, the High Court discussed how incompatibility issues might prevent a judge from exercising non-judicial functions even when that function was conferred persona designata and by consent in *Grollo v. Palmer*. The incompatibility condition stipulates that… 'no function can be conferred that is incompatible either with the judge's performance of his or her judicial functions or with the proper discharge by the judiciary of its responsibilities as an institution exercising judicial power'.[21] In relation to State judicial officers, see further the decision of *Kable v DPP (NSW)* (1996) 189 CLR 51.

Item 5 inserts **new section 6EB** into Part 1A of the Act, which defines *stored communications warrant information* to mean information about an application for, the issue of, the existence or non-existence of, or the expiry of a stored communications warrant, or any other information which is likely to identify the telecommunications service, or the person of interest, to which a stored communications relates. Stored communications warrant information is subject to a general prohibition against disclosure in **new section 133** of the Act.

This definition is based on the definition of designated warrant information in **section 6E** and is intended to ensure that information about agency investigations is not disclosed.

Items 6, 7 and 8 insert **new subsections 9(1A), 9A(1A)** and **10(1A)** which will allow the ASIO to access stored communications in the same manner it is able to intercept communications under a telecommunications service warrant or a named person warrant under the warrant regime in existing Chapter 2 of the Act, or warrant issued by the Director-General of Security in the emergency circumstances to which section 10 of the Act apply.

Item 9 introduces **new Chapter 3** into the Act, which establishes the general prohibition on accessing stored communications, the warrant regime exception for enforcement agencies and the accountability and oversight mechanisms.

The Explanatory Memorandum notes that with the introduction of the stored communications regime, the Act is to be restructured into Chapters to deal with interception and stored communications separately, although many provisions are mirrored.[22] Part 2 of Schedule 1 to the Bill contains many technical amendments to the Act to reflect this new structure.

Prohibition on access to stored communications

New Part 3-1 creates a general prohibition on access to stored communications and includes a number of exceptions to this general prohibition.

New section 108 creates a general prohibition on access to stored communications reinforced by an offence, punishable by imprisonment for up to two years or a fine of 120 penalty units or both, of accessing a stored communication without the knowledge of the intended recipient of the communication. The offence extends to accessing that communication, authorising, suffering or permitting another person to access that communication, or doing any act or thing which enables another person to access a stored communication.

The Explanatory Memorandum notes:

> This offence reflects the offence of intercepting a communication as set out in section 7, while reiterating the requirement that the conduct be done without the knowledge of the intended recipient. Importantly, the penalty for the commission of this offence is the same as the penalty for the unlawful interception of a communication, illustrating that the unauthorised access of the content of a person's communication is equally serious, regardless of the method of access.[23]

New subsection 108(2) sets out a number of exceptions to this general prohibition:

- where the access is authorised by a stored communications warrant
- where the access is authorised by an interception warrant
- where the conduct is done pursuant to a warrant issued under section 25A of the *Australian Security and Intelligence Organisation Act 1979*
- where the conduct is done by an employee of a carrier in the course of his or her duties, and where that conduct is reasonably necessary to perform those duties effectively
- where the conduct is done by a person as part of the installation, connection or maintenance of equipment, and where that conduct is reasonably necessary to perform those duties effectively
- where the conduct is done by a person as part of the installation, connection or maintenance of equipment to be used to access stored communications under a stored communications or interception warrant, where that conduct is reasonably necessary to perform those duties effectively; or
- where the access results from, or is incidental to, the actions of an employee of ASIO in lawfully determining the existence and location of a particular listening device.

New subsection 108(3) clarifies that an interception warrant only authorises access to stored communications (the exception set out in new paragraph (2)(b)), where the interception of the communication would have been authorised by the interception warrant, had that warrant been in effect at the time the communication was sent.

New subsection 108(4) provides that, in determining whether conduct was reasonably necessary for a person to perform his or her duties effectively, a court is to have regard to such matters (if any) as are specified in the regulations.

Access by ASIO to stored communications

New Part 3-2 inserts **new section 109** which ensures that ASIO is able to use its existing telecommunications interception warrants to obtain access to stored communications. Under the existing Chapter 2 of the Act, the Attorney-General may issue warrants to ASIO to intercept communications where the communications are being used by a person who is reasonably suspected of engaging in activities prejudicial to security, and the interception will, or is likely to, assist ASIO in its function of obtaining intelligence relevant to security.[24]

The Explanatory Memorandum notes:

> Any new warrant regime which would permit the Organisation to access stored communications would still require the Attorney-General to be the issuing authority, would still need to have the person of interest reasonably suspected of engaging in activities prejudicial to security and would still need to be likely to assist the Organisation in its function of obtaining intelligence relevant to security. As this is the same threshold as is currently required for an interception warrant, and interception warrants permit access to stored communications, there is no need for a separate stored communications warrant for the benefit of the Organisation.[25]

Access by enforcement agencies to stored communications

New Part 3-3 sets out the warrant regime for enforcement agencies to access stored communications. The provisions mirror existing Part VI of Chapter 2 of the Act which permits law enforcement agencies to intercept telecommunications.

However, as the Explanatory Memorandum states, unlike ASIO, enforcement agencies will obtain a clear benefit from a separate warrant regime to access stored communications. Key differences are set out at p. 12:

> - Additional agencies can obtain access. Only law enforcement agencies, being those agencies specifically tasked to investigate criminal matters (including the Australian Federal Police, the Australian Crime Commission, the Police Forces of each State and Territory, and various other criminal investigatory bodies investigating serious crime and corruption), are able to obtain interception warrants. However, stored communications warrants may be accessed by all enforcement agencies as defined in section 282 of the *Telecommunications Act 1997*, which includes all the law enforcement agencies, as well as all agencies responsible for administering a law imposing a pecuniary penalty or administration of a law relating to the protection of the public revenue. This will include such additional Commonwealth agencies as the

> Australian Customs Service, the Australian Tax Office, and the Australian Securities and Investments Commission. Similar State and Territory agencies are also included.
>
> - There is a wider range of issuing authority. Whereas interception warrants may only be issued by eligible judges or nominated AAT members, stored communications warrants may be also be issued by these authorities as well as any other Commonwealth, State or Territory judge or magistrate.
>
> - There is a lower threshold to be met. Interception warrants are only available in relation to specified serious offences, as defined in subsection 5(1). While these are varied in terms of their penalties, the general rule is that they relate to offences with a maximum term of imprisonment of at least seven years. In contrast, stored communications warrant are available for the investigation of these serious offences as well as offences with a penalty of imprisonment for a maximum period of at least three years or a pecuniary penalty of at least 180 penalty units for individuals and at least 900 penalty units for corporations.
>
> - In addition, stored communications warrants can be obtained as part of statutory civil proceedings which would render the person of interest to a pecuniary penalty of at least 180 penalty units for individuals and at least 900 penalty units for corporations. Consistent with the lower threshold, stored communications that have been lawfully accessed can be used as part of the investigation of matters with a lower threshold (at least one year imprisonment or at least 60 penalty units for individuals (300 penalty units for corporations).
>
> - Reflecting the wider agency access and the lower threshold to be met, the reporting requirements for stored communications warrant are not as burdensome on the agencies as the requirements for interception. Reduced reporting requirements are also consistent with general search warrants provisions. (emphasis added)

New Division 1 of new **Part 3-3** sets out the requirements for a valid application by an enforcement agency to an issuing authority for a stored communications warrant.

New section 110 provides that in the case of an interception agency, a warrant may be applied for by those officers or members of the agency that may apply for a telecommunications interception warrant (see existing section 39 of the Act).

In relation to other enforcement agencies, an application for a stored communications warrant may be made by a chief executive officer or person acting in that position, or a person nominated by the chief executive officer.

New section 110 provides that an agency may apply for a warrant authorising access to stored communications in respect of a person, similar to named person interception warrant. A stored communications warrant may authorise access to stored communications in relation to more than one telecommunications service. The Explanatory Memorandum gives as an example that a stored communications warrant may authorise access to all

SMS messages sent to and from a specified mobile telephone number and all emails sent to and from a specified email address.[26]

New sections 111 to 115 deal with the form of the warrant. The warrant must be in writing unless, because of urgent circumstances, the applicant thinks it necessary to apply by telephone with reasons for the urgency (**new sections 111 and 114**); the application must state the name of the agency and applicant (**112**); the matters that must be included in an affidavit in support of an application for a stored communications warrant are set out, including the facts or grounds on which the application is based (**113**).

New section 115 provides the issuing authority with the power to request further information, and the form in which the further information must be given.

New section 116 mirrors section 46 of the existing Act in relation to the issue of interception warrants. It provides that an issuing authority may issue a stored communications warrant if he or she is satisfied of the following matters:

- that the administrative requirements set out in new sections 110 to 115 have been complied with
- where the application was made by telephone, that the urgency of the situation justified a telephone application
- that there are reasonable grounds for suspecting that a particular carrier holds stored communications for whom the identified person is the sender or the intended recipient
- that information that could be obtained from those stored communications would be likely to assist in the investigation of a serious contravention;[27] and
- having regard to the matters listed in new subsection (2), and no other matters, that a stored communications warrant should be issued.

New subsection 116(2) provides an exhaustive list of the matters that an issuing authority can consider, which are the same as the matters that can be considered in relation to an interception warrant. They include the impact on privacy, the gravity of the serious contravention, the likely value of the information that could be obtained and a comparison of other methods of investigation.

New section 117 confirms that a stored communications warrant authorises access to stored communications for persons approved under **new subsection 127(2)** to stored communications that came into existence before the warrant is first issued and that are still held by the carrier.

New section 118 states the requirements for the form and content of a stored communications warrant. **New section 119** provides the time for which a stored communications warrant is in force. This is until it is first executed, or five days after the day of which it was issued, whichever occurs first, per communications carrier. The period

cannot be extended (**new subsection 119(3)**), but a further warrant can be issued in respect of the same person after a delay of three days (**subsections 119(4) and (5)**).

Sections 120 to 124 in a **new Division 3** of new Part 3-3, contain provisions dealing with notification and revocation of stored communications warrants.

Sections 125 to 132 in a **new Division 4** of new Part 3-3, sets out other provisions relating to the authority conferred by warrants. **New section 132** creates an offence of obstructing or hindering, without a reasonable excuse, a person acting under the authority of a stored communications warrant. The offence is punishable by imprisonment for 6 months, or 30 penalty units, or both.

Dealing with accessed information

New Part 3-4 provides a general prohibition against dealing with accessed information, subject to some permitted dealings. It also includes provisions relating to the admissibility of evidence and the destruction of records. **New section 133** creates a general offence for communicating, making use of, making a record of or giving as evidence, lawfully accessed information, or information obtained by accessing a stored communication in contravention of new section 108 or stored communications warrant information. The penalty for this offence is imprisonment for two years, 120 penalty units, or both, which is uniform with the twin offence for interception.

New Division 2 of new Part 3-4 provides the following exceptions to the prohibition on dealing with accessed information:

- for the purposes of applying for, or being issued, a stored communications warrant
- for permitting inspection of stored communications warrants
- for making reports to the Minister about stored communications warrants **(new section 134)**
- for an employee of a carrier to provide the information to the agency in relation to whom a warrant has been issued, to assist with the operation of a network or to assist in lawful access to a stored communication (**new section 135**)
- in connection with the performance by ASIO of its functions **(new section 136)**
- for the purposes of communicating information obtained by ASIO (**new section 137**)
- for an employee of a carrier, to communicate accessed information to an enforcement agency for the purposes of an investigation of a serious offence, and for no other purpose (**new section 138**)
- to communicate, use or record accessed information for the purposes of an investigation by the agency of a contravention which is a serious offence, or is

punishable by a maximum period of at least 12 months or by a maximum fine of at least 60 penalty units (**new section 139**)

- for a person to communicate accessed information to the Attorney-General, Director of Public Prosecutions, Commissioner of the Australian Federal Police, or Chief Executive Officer of the Australian Crime Commission if the information is believed to establish that a particular offence has been committed (**new section 140**)
- to give lawfully accessed information and stored communications warrant information in evidence in an exempt proceeding (**new section 143**) *Exempt proceeding* is defined in section 5B of the Act. There is discretion to admit unlawfully accessed stored communications information into evidence in an exempt proceeding where the accessed information was purportedly under an irregular stored communications warrant under **new section 144**.[28]

New subsection 150(1) requires the chief officer of an enforcement agency to cause the destruction of information or a record obtained by accessing a stored communication. This is where the chief officer is satisfied that the material is no longer required in relation to the purposes of the agency providing an annual report on destruction activity to the Minister referred to in **new subsection 150(2)**.

Keeping and inspection of access records

New Part 3-5 establishes an oversight regime for the records to be maintained by enforcement agencies in connection with the use of stored communications warrants.

New section 151 requires the chief officer of an enforcement agency to cause to be kept in the agency's records, each stored communications warrant obtained by the agency, and each revocation instrument, evidentiary certificate, and authorisation in relation to the warrant. Further, the records must include particulars of the destruction of information obtained pursuant to the warrant.

New section 152 in **new Division 2,** provides that the Ombudsman can inspect an enforcement agency's records in order to ascertain compliance with its record-keeping obligations, and can do anything incidental or conducive to that function.

New subsections 153(1) and (2) provide that within three months of the end of each financial year the Ombudsman will report to the Minster about the inspections conducted during the financial year of an enforcement agency's stored communications records. **New subsection 153(4)** provides the Ombudsman with an ability to report to the Minister at any time about the results on an inspection under this new Division, and must do so if requested by the Minister. **New subsection 153(3)** provides that the Ombudsman may report to the Minister any contravention of a provision of this Act

New subsection 153(5) obliges the Ombudsman to provide a copy of a report under subsections 153(1) or (3) to the chief officer of the relevant enforcement agency.

New section 154 confirms the general powers of the Ombudsman in relation to inspections as provided by the *Ombudsman Act 1976* but they remain subject to section 133 of the Act which provides a general prohibition against dealing with accessed information or stored communications warrant information.

New section 155 provides that the general prohibition against dealing with accessed information or stored communications warrant information does not prevent the disclosure of information to the inspecting officer for the purposes of an inspection under this new Part, nor does section 133 prevent making a record of the information for that purpose.

New section 156 provides that an inspecting officer may use, record or communicate information for the purposes of an inspection of an enforcement agency's records despite section 133 of the Act.

New subsection 157(1) provides that section 11A of the *Ombudsman Act 1976* – regarding the power of the Federal Court of Australia to determine matters of the Ombudsman's powers – does not apply to the proposed exercise of a power or function by the Ombudsman under this new Division.

New subsection 157(2) provides that section 19 of the *Ombudsman Act 1976* – regarding annual reporting to Parliament – does not apply to any act or omission of an inspecting officer under this new Division. However, **new subsection 157(3)** provides that subsection 35(2), (3), (4) and (8) of that Act dealing with the confidentiality requirements for inspecting officers do apply for the purposes of this Division (subject to new section 155).

New section 158 provides that the Ombudsman may give or receive information to those State inspecting authorities that have the function of inspecting the individual enforcement agency's compliance with the telecommunications interception regime. The effect of this provision is to enable the Ombudsman to communicate any accessed information to a State inspecting authority if it is relevant to the performance of the State inspecting authority's functions.

Reports about access to stored communications

New Part 3-6 imposes requirements on enforcement agency's to provide an annual report to the Minister regarding the use of stored communications warrants.

New Division 1, new section 159 obliges the chief officer of an enforcement agency to provide the Minister with a report on the use of stored communications warrants. The information required is set out in **new Division 2** of this Part. The report must be provided within three months after the end of each financial year.

New section 160 provides that the Minister may seek information from the chief officer of an enforcement agency additional to that provided under new section 159. To the extent that it is practicable, the chief officer must comply with the request of the Minister.

New Division 2, new section 161 requires the Minister to cause to be prepared an annual report regarding the use of stored communications warrants in each financial year. The information to be included in this annual report is set out in **new section 162**; including

- for each enforcement agency, the statistics on how many stored communication warrant applications were made, and how many applications were made by telephone
- statistics for each enforcement agency regarding the number of arrests made on the basis of accessed information or the number of proceedings that ended during the reporting year in which accessed information was used, and
- a total figure for all enforcement agencies regarding how many stored communication warrant applications were made, how many applications were made by telephone, how many renewal applications were made, and how many stored communications warrants were issued with conditions or restrictions.

New Division 3, new section 164 obliges the Minister to table the annual report before each House of the Parliament within fifteen sitting days of its preparation.

Civil remedies

New Part 3-7 provides the same civil remedies for unlawful access to stored communications and unlawful disclosure of accessed information as are available for unlawful interception under Chapter 2 of the Act.

New section 165 provides that an aggrieved person – a party to the communication or a person on behalf of whom the communication was made – may apply for civil remedial relief against a person who unlawfully accessed the relevant communication. **New subsection 165(7)** provides a list of orders that may be made upon application for relief. A criminal court may also provide criminal remedial relief upon application of an aggrieved person if the court convicts a person of unlawful access.

New section 165 further provides that an aggrieved person may apply for civil remedial relief for communication of the accessed information. A criminal court may also provide criminal remedial relief upon application of an aggrieved person if the court convicts a person of unlawful communication of accessed information.

New subsection 165(11) provides that the section does not apply to unlawful access that occurred as a result of a defect or irregularity in connection with the stored communications warrant documentation or the execution of the warrant.

New section 166 provides the limitation periods in respect of remedial relief – six years after the unlawful access or unlawful communication. An application for criminal court relief must be made as soon as practicable after the conviction occurred.

New section 167 provides that this new Part does not limit the criminal or civil liability of a person under any other law. Further, the section provides for an aggrieved person to seek remedial relief in relation to an offence arising out of this Act.

New section 168 preserves the operation of any law of a State or Territory that is capable of operating concurrently with this Part. For example, any State or Territory legislation that seeks to regulate lawful access to communications held other than by a carrier, is preserved by the section to the extent that it is able to operate concurrently.

New section 169 clarifies that nothing in this new Part enables an inferior court of a State or Territory to grant remedial relief that it is otherwise unable under the laws of that State or Territory to provide.

New section 170 overrides section 19B of the *Crimes Act 1914* so that remedial relief is available from a criminal court once a defendant has been convicted of unlawful access or unlawful communication, even if the court proceeds not to record a conviction.

New Part 2 includes amendments that are consequential upon the change of name of the Act to the *Telecommunications (Interception and Access) Act 1979*, and the inclusion of new definitions and concepts from this Bill into cross-referenced sections of other legislation.

Schedule 2 — B-party interception

Item 1 inserts a **new subparagraph 9(1)(ia)** into the Act which will allow the Attorney-General to issue a warrant under existing section 9 to ASIO which authorises the interception of the means by which a person receives or sends a communications from or to another person who is engaged in, or reasonably suspected by the Director-General of Security of being engaged in, or of being likely to engage in such activities.

Items 4 and 5 amend subsection 9B(3) to provide that the time period for a B-Party warrant issued to ASIO by the Attorney-General must not exceed 3 months. **Item 10** would amend existing subsection 49(3) to provide that the time period for a B-Party warrant issued to the agency by an eligible judge or nominated AAT member must not exceed 45 days.

Item 6 amends existing subsection 46(1) to provide that the preconditions in paragraphs (a) to (c) must each be separately met prior to the issue of an interception warrant.

Item 7 amends existing subsection 46(1) of the Act to provide that a telecommunications service warrant can be issued in relation to a person who is involved in the commission of an offence, or a person who communicates with such a person.

Items 8 and 9 insert a **new subsection 46(3)** which provides that an eligible judge or nominated AAT member must not issue a telecommunications service warrant for a B-Party warrant unless he or she is satisfied that the agency has exhausted all other practicable methods of identifying the telecommunications services used, or likely to be used, by the person involved in the serious offence or serious offences, or where the interception of a telecommunications service used, or likely to be used by that person, is not practicable.

The Explanatory Memorandum notes that:

> This means that, for example, where an undercover police operative is provided a mobile handset to communicate with the suspect by the suspect and the interception of the suspect's services is not practical because the service cannot be readily identified. The telecommunications of the undercover operative would be able to be intercepted under section 46.[29]

Schedule 3 – Equipment-based interception

Item 2 inserts a definition of *telecommunications device* into the Act. Telecommunications device means 'a terminal device that is capable of being used for transmitting or receiving a communication over a telecommunications system'.

The Explanatory Memorandum states that a terminal device is 'any end piece of telecommunications equipment by which a person may communicate, including a mobile handset, personal computer, or personal digital assistant', but it is not currently defined in the existing Act or current Bill.[30]

Item 3 inserts a definition of *telecommunications number* into the Act. The telecommunications number is a means by which interception agencies may identify the telecommunications device which is to be the subject of an interception warrant.

The Explanatory Memorandum states:

> A telecommunications device may be identified by any unique number including a telephone number for mobile phone handsets, a Media Access Control address for computer terminals, or an e-mail address. The definition of telecommunications number is inclusive so as not to limit the unique numbers which may be used to identify telecommunications devices, thereby maintaining a technology neutral approach to the regulation of telecommunications interception.[31]

Item 4 provides that a telecommunications device may be identified by a unique telecommunications number or any other unique identifying factor.

Item 5 repeals and substitutes existing subsection 9A(1) of the Act to include interception on the basis of a telecommunications device. This subsection provides that the Attorney-General may issue a named person warrant to ASIO for the purposes of obtaining intelligence in relation to security.

Item 7 requires that the Director-General of Security include in an application for a warrant under section 9A a description of the telecommunications device sufficient to identify the telecommunications device used or likely to be used by the person of interest. The telecommunications device may be described by reference to a unique telecommunications number of other unique number.

Item 8 provides that before issuing a warrant to intercept a device to ASIO, the Attorney-General must be satisfied that ASIO has no practicable methods of identifying the telecommunications service to be intercepted at the time of the application, or that interception of the telecommunications service would be impracticable.

Item 9 repeals and substitutes existing subsection 11B(1) of the Act to include interception on the basis of a telecommunications device. Section 11B allows the Attorney-General to issue a named person warrant to the Organisation for the purposes of obtaining foreign intelligence relating to a matter specified in the notice. As per Items 7 and 8, **Item 11** requires that the Director-General of Security include in an application for a warrant under 11B a description of the telecommunications device sufficient to identify the telecommunications device, which may be a unique number; and **Item 12** provides that the Attorney-General must be satisfied that ASIO has no practicable methods of identifying the telecommunications service to be intercepted at the time of the application, or that interception of the telecommunications service would be impracticable.

Item 13 amends the notification requirements in section 16 of the Act to remove the requirement to identify the telecommunications service to be intercepted when applying for named person warrants.

Item 14 amends the notification requirements in section 16 of the Act to oblige a certifying person of ASIO to provide the Managing Director of a carrier with a written description sufficient to identify any telecommunications device to be intercepted if that telecommunications device is not identified on the warrant. This provision recognises that named person warrants may authorise interception of multiple telecommunications devices. **Items 15 and 16** further oblige a certifying officer of ASIO to inform the Managing Director of a carrier where the Director-General is satisfied that interception of a telecommunications device is no longer required.

Items 22 to 24 make the same amendments to notification requirements in section 60 of the Act.

Item 20 repeals and substitutes paragraph 46A(2)(a) of the Act which requires the issuing authority to have regard to the interference with the privacy of the person of interest by authorising interception of the person's services 'or telecommunications devices'.

Item 21 adds the criteria outlined in **item 7** for an interception agency when seeking interception on the basis of a telecommunications device operated by the person of interest.

Schedule 4 – Class 1 and Class 2 offences

The Explanatory Memorandum notes in relation to this Schedule:

> The amendment will require the issuing of all interception warrants to have regard to privacy considerations. Previously, only class 2 interception warrants required an eligible judge or nominated AAT member to have regard to the privacy considerations.
>
> These amendments are designed to simplify a complex area of the interception regime and enhance the privacy underpinnings of the Act.[32]

Items 1 and 2 repeal the definitions of class 1 and class 2 offences in subsection 5(1) to reflect the insertion of a new definition of serious offence. The new definition of serious offence will incorporate all offences defined as class 1 and class 2 offences.

Items 3 to 12, and **Items 14 to 20** make consequential amendments to the Act to reflect the amendment.

Item 13 inserts a new subsection 5D(7) which ensures that it is a serious offence for the purposes of the interception regime if an offence is constituted by receiving or assisting a person who is, to the offender's knowledge, guilty of a serious offence, which was previously a class 1 offence as outlined in subsection 5D(1), in order to enable the person to escape punishment or to dispose of the proceeds of the offence.

Items 31 to 34 are transitional provisions that save the validity and operation of warrants issued under sections 45, 46 and 48.

Schedule 5 – Transfer of functions

The Blunn Report recommended the removal of the Telecommunications Interception Remote Authority Connection (TIRAC) function exercised by the Telecommunications Interception Division of the Australian Federal Police (AFP) from the Act. The proposed amendments would also transfer the function of compiling the registers to the Secretary of the Attorney-General's Department.

The Explanatory Memorandum states:

> TIRAC is a historical electronic accountability mechanism which requires each interception agency to lodge its interception warrants with the AFP. The effect of this function is that the warrants do not take effect until the AFP receives the warrant and notifies the Managing Director of the carrier of the issue of the warrant. TIRAC's utility has been exhausted by technological developments, and it is therefore proposed that it be removed from the Act.
>
> The proposed amendments will continue to require all agencies to maintain comprehensive records as part of the interception regime, however, interception agencies will no longer be required to notify the AFP of the issue of the warrant before it takes effect.[33]

Item 5 removes the reference to the AFP in subsection 52(2). The effect of the item is to notify the Secretary of the Department of a proposed revocation and provide a copy of that revocation to the Secretary of the Department.

Item 6 amend paragraphs 52(2)(a) and (b) to transfer the requirement to notify the Commissioner of Police about the issue of an interception warrant to the Secretary of the Department.

Item 7 omits reference to the AFP in subsection 53(1) thereby requiring all interception agencies, including the AFP to notify the Secretary of the Department of the issue of a telecommunications interception warrant.

Item 8 would amend paragraphs 53(1)(a), (b) and (c) to transfer the requirement to notify the Commissioner of Police about the issue of an interception warrant to the Secretary of the Department.

Items 11 and 12 amend existing subsections 57(1) and (2), and paragraphs 57(3)(a) and (b) to transfer the requirement to notify the Commission of Police regarding the revocation of a warrant to the Secretary of the Department.

Items 16 and 17 amend section 59 and paragraph 60(2)(a) to transfer the requirement to notify the Commission of Police regarding the revocation of a warrant to the Secretary of the Department.

Items 25 and 29 are saving provisions which preserve the General Register of Warrants and the Special Register of Warrants maintained by the Commissioner of Police as the General Register of Warrants and the Special Register of Warrants maintained by the Secretary of the Department after the commencement of this item.

Schedule 6 – Other amendments

Item 1 would amend the definition of 'permitted purpose' of the Act by amending subparagraph 5(1)(f)(ii). A 'permitted purpose' in the case of the Office of Police Integrity will mean a purpose connected with an investigation by the Director, Police Integrity under the Victorian *Police Regulation Act* or the *Whistleblowers Protection Act*, into serious misconduct (which includes corrupt conduct), together with any report on such an investigation.

The Explanatory Memorandum states:

> This means that, under section 67 of the Act, the Director, Police Integrity may disclose lawfully intercepted information to another person but only for a purpose connected with an investigation by the Director, Police Integrity under the Police Regulation Act or the Whistleblowers Protection Act into the conduct of a member of the force or into serious misconduct (which includes corrupt conduct), together with any report on such an investigation.[34]

In September 2005 the Commonwealth and Victorian governments resolved a dispute over access by the Victorian Office of Police Integrity to telecommunications interceptions, including phone tap powers. The Office of Police Integrity was established in November 2004 by the Victorian Government to combat police corruption and serious misconduct. The Victorian Ombudsman, George Brouwer, was appointed to run the new body at the same time as continuing in his role as Ombudsman. The Federal Government initially refused to grant the new body telecommunications interception powers, arguing that Mr Brouwer would have a conflict of interest since one of his functions as Ombudsman is to oversee and investigate complaints about use of such powers.

Item 4 amends paragraph 5D(4) to update the reference to the New South Wales money laundering offences to which an interception agency can apply for an interception warrant. Due to a legislative change in New South Wales, the money laundering offences were relocated from the *Confiscation of Proceeds of Crime Act 1989* (NSW) into the *Crimes Act 1900* (NSW).

Item 5 will repeal subsection 6(2). Section 6(2) creates an exception to the general prohibition in subsection 7(1) against the interception of a communication in its passage over the Australian telecommunications system. At the commencement of the Act, subsection 6(2) was intended to exempt the activities of telecommunications carriers and employees of carrier from the general prohibition contained in subsection 7(1) to allow the testing of the carrier's equipment to ensure that the telecommunications network and associated equipment operated correctly. The Explanatory Memorandum states that subsection 6(2) 'no longer has application in the deregulated telecommunications market and its continued application undermines the strict privacy protections contained in the Act is based'.[35]

Items 7 and 9 correct drafting errors within the Act which have been the result of previous amendment Acts.

Item 8 amends subsection 55(5) of the Act to clarify and make retrospective that an employee of a carrier can provide technical assistance to a law enforcement agency, or officer, when such an agency or officer is executing an interception warrant on a carrier and throughout the consequent interception. This amendment was necessary in light of the decision of the South Australian District Court in the case of *R v Sutton and Rodgers* (Simpson J, District Court of South Australia, unreported, 10 February 2003).

Concluding Comments

The TI Act did need revision to keep up to date with technological advances. The move to provide specific warrants for stored communications is welcome, if possibly overdue, as it had been argued strongly in the Senate that privacy concerns were not appropriately addressed by ordinary search warrants.

Electronic Frontiers Australia stated in relation to the 2002 Bill that:

> The changes are the same as deciding that postal mail remains protected from interception while being delivered by the postman and transported in Australia post vehicles, but not while stored in Australia Post premises awaiting delivery.[36]

However, it could be argued that the wider and easier access of enforcement agencies to stored communication is unwarranted (note discussion of **new Part 3.3** above). As the Explanatory Memorandum states, enforcement agencies will obtain a clear benefit from a separate warrant regime to access stored communications. Key differences are set out at p. 12:

- Additional agencies can obtain access. Only law enforcement agencies, being those agencies specifically tasked to investigate criminal matters (including the Australian Federal Police, the Australian Crime Commission, the Police Forces of each State and Territory, and various other criminal investigatory bodies investigating serious crime and corruption), are able to obtain interception warrants. However, stored communications warrants may be accessed by all enforcement agencies as defined in section 282 of the *Telecommunications Act 1997*, which includes all the law enforcement agencies, as well as all agencies responsible for administering a law imposing a pecuniary penalty or administration of a law relating to the protection of the public revenue. This will include such additional Commonwealth agencies as the Australian Customs Service, the Australian Tax Office, and the Australian Securities and Investments Commission. Similar State and Territory agencies are also included.
- There is a wider range of issuing authority. Whereas interception warrants may only be issued by eligible judges or nominated AAT members, stored communications

warrants may be also be issued by these authorities as well as any other Commonwealth, State or Territory judge or magistrate.

- There is a lower threshold to be met for stored communication warrants versus interception warrants. Interception warrants are only available in relation to specified serious offences, as defined in subsection 5(1). While these are varied in terms of their penalties, the general rule is that they relate to offences with a maximum term of imprisonment of at least seven years. In contrast, stored communications warrant are available for the investigation of these serious offences as well as offences with a penalty of imprisonment for a maximum period of at least three years or a pecuniary penalty of at least 180 penalty units for individuals and at least 900 penalty units for corporations.
- stored communications warrants can be obtained as part of statutory civil proceedings which would render the person of interest to a pecuniary penalty of at least 180 penalty units for individuals and at least 900 penalty units for corporations. Consistent with the lower threshold, stored communications that have been lawfully accessed can be used as part of the investigation of matters with a lower threshold (at least one year imprisonment or at least 60 penalty units for individuals (300 penalty units for corporations)
- reporting requirements for stored communications warrant are not as burdensome on the agencies as the requirements for interception.

The presumption is that a communication is less private because it is in an unread email, voicemail or text rather than verbally delivered over the phone. One issue is whether the range and threshold of access should be lowered and reporting made less onerous because of the technical difference that a communication has already passed over a carrier. There is also the key public policy issue about whether information obtained this way should be admissible in a civil proceeding.

The added privacy protection given to more traditional methods of communication may be the product of generational custom rather than logic. It is questionable whether young Australians would see text messages and emails as less private than live phone conversations or the postal service.

The changes to B-Party intercepts may be seen as simply clarifying the circumstance argued in the *Flanagan* case in the Federal Court, discussed above, or it may be seen as introducing an intrusive new power that unnecessarily erodes the privacy of innocent third parties.

The amendments relating to Schedule 4 serious offences can be seen as beneficial legislation as they add privacy considerations to the list of issues an issuing authority can consider.

The Bill has raised considerable anxiety in the press and minority parties which may be attributable to wider concerns about government surveillance of Australian citizens and

privacy issues. The Attorney-General referred a review of the *Privacy Act 1988* to the Australian Law Reform Commission (ALRC) on 31 January 2006 with a final report due by 31 March. The ALRC should have regard to:

> the rapid advances in information, communication, storage, surveillance and other relevant technologies
>
> possible changing community perceptions of privacy and the extent to which it should be protected by legislation
>
> the expansion of State and Territory legislative activity in relevant areas, and
>
> emerging areas that may require privacy protection.[37]

Finally, this Bill was introduced on 15 February 2006 and is listed for debate in the House of Representatives on 28 February 2006. Parliament may wish to consider whether Bills of this type which have considerable technical detail and raise ongoing issues of debate, such as privacy rights, might require more time for consideration by Members.

Endnotes

1 Explanatory Memorandum, at pp. 1–2.

2 The Telecommunications (Interception) Amendment (Stored Communications) Bill 2004 was originally introduced on 27 May 2004. This Bill lapsed when the 40th Parliament was prorogued for the October 2004 general election. The Bill was re-introduced in identical form on 17 November 2004.

3 Tom Allard and Louise Dodson, 'Proposed phone-tapping powers come under fire from all sides', *Sydney Morning Herald*, 16 February 2006, p. 4.

4 Anthony Blunn, August 2005.

5 ibid, at p. 75.

6 ibid, at p. 77.

7 Flanagan, at pp. 201–2.

8 *Flanagan v AFP* (1996) 60 FCR 149 at p. 76.

9 Blunn, op cit, at p. 76.

10 Explanatory Memorandum, at p. 34.

11 ABC Radio, 'Civil liberties spokesperson discusses proposed changes to telecommunications interception laws', *AM*, 15 February 2006.

12 Mike Jeffreys, 'Civil libertarians are alarmed at new police phone tap powers', *Radio 2CC*, 16 February 2006.

13 Brendan Nicholson, 'Proposal to tap innocent people 'unwarranted', *The Age*, 16 February 2006, p. 6.

14 NSW Council of Civil Liberties, 'Australian phones 26-times more likely to be bugged than an American phone', *media release*, 13 January 2006. Making AAT Members issuing authorities in 1999 were also blamed for the increase by ALP Daryl Melham in 2002. A spokesman for Mr Melham said 'This has meant [there is] a bigger pool of people ready 24 hours a day, signing off warrants, and [they're] signing off virtually automatically'. Cynthia Banham, 'Rampant phone tapping puts US in the shade', *Sydney Morning Herald*, 16 September 2002.

15 Tom Allard and Louise Dodson, 'Proposed phone-tapping powers come under fire from all sides', *Sydney Morning Herald*, 16 February 2006, p. 4.

16 Arch Bevis MP, Senator Joe Ludwig, and Nicola Roxon MP, 'Telecommunications Interception Bill', *Joint Statement*, 15 February 2005.

17 Senator Natasha Stott Despoja, 'Democrats challenge privacy violations', *media release*, 15 February 2006.

18 Senator Bob Brown (Australian Greens), 'Phone taps cross the line', *media release*, 15 February 2006.

19 Explanatory Memorandum, at p. 7.

20 Explanatory Memorandum, at pp. 7–8.

21 (1995) 184 CLR 348 at 364–5.

22 Explanatory Memorandum, at p. 9.

23 Explanatory Memorandum, at p. 10.

24 Note also that the test for a general search warrant or computer access warrant under sections 25(5) or 25A of the ASIO Act is if the Minister is satisfied that there are reasonable grounds for believing that access by ASIO to records or other things on particular premises or computer will substantially assist the collection of intelligence in accordance with the ASIO Act in respect of a matter that is important in relation to security (subsection 25(2)). Under the general search warrant power contained in paragraph 25(4)(d), ASIO can remove and retain records for the purposes of making copies or inspecting the record.

25 Explanatory Memorandum, at p. 11.

26 Explanatory Memorandum, at p. 13.

27 New subsection 116(3) clarifies that a stored communications warrant may be issued in relation to the investigation of more than one serious contravention.

28 The Federal Court case of *Carmody v MacKellar* (1997) 148 ALR 210 held that the *Telecommunications (Interception) Act 1979* was an example of a statutory power which can override legal professional privilege because of the powers to listen to and record live communications. The amendments to the *TI Act 1979* preserve the rule that communications which are subject to legal professional privilege cannot be adduced in evidence, even if lawfully intercepted: see *TI Act*, subs 74(1) and s 78.

29 Explanatory Memorandum, at p. 33.

30 Explanatory Memorandum, at p. 34.

31 Explanatory Memorandum, at p. 35.

32 Explanatory Memorandum, at p. 39.

33 Explanatory Memorandum, at p. 42.

34 Explanatory Memorandum, at p. 33.

35 Explanatory Memorandum, at p. 48.

36 EFA, Telecommunications Interception Legislation Amendment Bill 2002, 29 July 2002, accessed 23 February 2006.

37 ALRC terms of reference can be found online at http://www.alrc.gov.au/inquiries/current/privacy/terms.htm.

Members, Senators and Parliamentary staff can obtain further information from the Information and Research Services on (02) 6277 2759.