2002-2003-2004

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT BILL 2004

EXPLANATORY MEMORANDUM

(Circulated by authority of the Attorney-General,
the Honourable Philip Ruddock MP)

TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT BILL 2004

OUTLINE

This Bill amends the *Telecommunications (Interception) Act 1979* (the Interception Act) to extend the availability of telecommunications interception warrants to additional serious offences, extend the protections of the Act in relation to text based communications, facilitate the recording of calls to publicly-listed ASIO numbers, and to clarify the application of the Act to delayed access message services.

Specifically, the Bill amends the Interception Act to:

- include terrorist offences set out in Divisions 72, 101, 102 and 103 of the Commonwealth *Criminal Code*, offences involving dealings in firearms and State and Territory cybercrime offences as offences in respect of which a telecommunications interception warrant may be sought,

- extend the definition of interception to include reading or viewing a communication,

- exclude from the definition of interception the act of listening to, recording, reading or viewing communications to publicly-listed ASIO numbers,

- clarify the application of the Act to delayed access messages services such as email and SMS messaging,

- remove the requirement for ASIO to notify the telecommunications carrier where a warrant has been issued for the interception of a telecommunications service operated by the carrier and the assistance of the carrier is not required in order to execute the warrant, and

- allow certifying officers to form the view that interception of a particular service is no longer required, thereby expediting the cessation of interception where it is no longer necessary.

FINANCIAL IMPACT STATEMENT

There are no direct financial impacts from this Bill.

NOTES ON CLAUSES

Clause 1: Short Title

Clause 1 is a formal provision specifying the short title of the Act.

Clause 2: Commencement

Clause 2 specifies the time at which the Bill commences, providing that the Act will commence on the day after it receives the Royal Assent.

Clause 3: Schedules

Clause 3 provides that each Act specified in a schedule is amended as set out in the schedule concerned.

Schedule 1 – General amendments

Telecommunications (Interception) Act 1979

Item 1

This item amends the definition of class 1 offence set out in subsection 5(1) of the *Telecommunications (Interception) Act 1979* (the Act) to include a new paragraph (cb). The new paragraph includes within the definition of class 1 offence a reference to offences against Divisions 72, 101, 102 and 103 of the *Criminal Code.*

Division 72 of the *Criminal Code* sets out offences relating to terrorist activities using explosive or lethal devices. Division 101 sets out terrorism offences, including engaging in a terrorist act, providing or receiving training connected with terrorist acts, possessing things connected with terrorist acts and making documents likely to facilitate terrorist acts. Division 102 sets out offences in relation to terrorist organisations, including directing the activities of a terrorist organisation, membership of a terrorist organisation and providing training to or receiving training from a terrorist organisation. Division 103 sets out an offence of providing or collecting funds to facilitate or engage in a terrorist act.

The effect of the amendment is to permit agencies to apply for a warrant authorising the interception of telecommunications where information that may be obtained would be likely to assist in the investigation of offences set out in Divisions 72, 101, 102 or 103 of the *Criminal Code*, thus ensuring the availability of telecommunications interception in connection with the investigation of the terrorism offences. This amendment supplements existing provision at paragraph (ca) of the definition of class 1 offence, which allows a telecommunications interception warrant to be sought in connection with the investigation of offences involving an act or acts of terrorism.

Item 2

This item amends paragraph (d) of the definition of class 1 offence in subsection 5(1) of the Act to replace the existing reference to paragraph (ca) of the definition with a reference to paragraph (ca) or (cb). The amendment is consequential upon the insertion of a new paragraph (cb) into the definition by item 1.

Item 3

This item amends the definition of class 2 offence set out in section 5D of the Act to replace the existing reference to armament dealings in subparagraph (3)(d)(x) with a reference to dealings in firearms or armaments. The amendment makes it clear that a warrant under Part VI of the Act may be issued to assist in the investigation of offences involving dealings in either firearms or armaments. The term “firearm” generically describes any weapon capable of propelling a projectile by means of an explosive. The ordinary meaning of the term “armaments” encompasses weaponry, munitions or other equipment of a military nature.

The effect of the amendment is to permit agencies to apply for a warrant authorising the interception of telecommunications where information that may be obtained would be likely to assist in the investigation of offences involving dealings in firearms or armaments in circumstances where the commission of the offence involves two or more offenders,

substantial planning and organisation, involves or ordinarily involves sophisticated methods and techniques and the relevant offence is punishable by a maximum of at least 7 years imprisonment. The amendment will ensure that intercepting agencies are able to seek interception warrants in connection with the investigation of firearms dealings in cases where the preconditions set out in subsection 5D(3) are met.

Item 4

This item amends the definition of class 2 offence set out in section 5D of the Act to replace the existing reference in subsection 5D(5) to offences against Part 10.7 of the *Criminal Code* with a broader list of cybercrime offences in Commonwealth, State and Territory legislation.

The effect of the amendment is to permit agencies to apply for a warrant authorising the interception of telecommunications where information that may be obtained would be likely to assist in the investigation of the computer offences listed in paragraphs (a) to (f) of the new subsection 5D(5). The amendment will allow intercepting agencies to seek interception warrants in connection with the investigation of the range of State and Territory offences referred to in the subsection in addition to the Commonwealth computer offences contained in Part 10.7 in the *Criminal Code*.

The new subsection 5D(5) includes separate references to cybercrime offences in New South Wales, Victoria, Western Australia and other states and territories because different cybercrime offences have been enacted in each of those jurisdictions. The provisions of the *Crimes Act 1900* (NSW) and *Crimes Act 1958* (Vic) referred to in new paragraphs 5D(5)(b) and 5D(5)(c) substantially mirror the provisions of Part 10.7 of the *Criminal Code*. New paragraphs 5D(5)(d) and 5D(5)(e) accommodate other states and territories that legislate in the future to mirror Part 10.7 of the Commonwealth *Criminal Code*.

Item 5

This item amends the definition of interception set out in subsection 6(1) to replace the existing reference to listening to or recording a communication with a reference to listening to, recording, reading or viewing a communication.

The amendment will have the effect of extending the definition of interception to include reading or viewing a communication in its passage over the telecommunications system, and consequently extending the prohibition against interception set out in subsection 7(1) of the Act. This will extend the protection afforded to communications in their passage over the telecommunications system to include protection from reading or viewing those communications. This extension addresses advances in technology which have resulted in many telecommunications now taking the form of written words, such as email, or even images and to which the concept of listening is not directly applicable.

Item 6

This item amends subsection 6(2) of the Act to replace existing references to listens to or records with references to listens to, records, reads or views. The amendment is consequential upon the extension to the definition of interception effected by item 5.

Item 7

This item amends subsection 6(2) of the Act to replace the existing reference to listening to or recording with a reference to listening to, recording, reading or viewing. The amendment is consequential upon the extension to the definition of interception effected by item 5.

Item 8

This item amends subsection 6(2B) to replace the existing reference to listens to or records with a reference to listens to, records, reads or views. The amendment is consequential upon the extension to the definition of interception effected by item 5.

Item 9

This item amends subsection 6(2B) to replace the existing reference to listening to or recording with a reference to listening to, recording, reading or viewing. The amendment is consequential upon the extension to the definition of interception effected by item 5.

Item 10

Communications to publicly-listed ASIO numbers

This item inserts two new subsections into section 6 of the Act to enable ASIO to listen to, record, read or view communications made to the Australian Security Intelligence Organisation (ASIO) via a publicly-listed number.

New subsection 6(3) defines a publicly-listed ASIO number as a telephone number that enables members of the public to contact ASIO and is listed in a telephone directory or telephone number database that is available to the public.

This item also inserts new subsection 6(4), which provides that in circumstances where a person makes a call to a publicly-listed ASIO number, the listening to, recording, reading or viewing of that communication by a person lawfully engaged in duties relating to the receiving and handling of calls to that number does not constitute an interception for the purposes of the Act. The effect of the amendment is to allow ASIO to record calls made to publicly-listed ASIO numbers. The amendment is limited to calls made to ASIO and does not extend to allowing the recording of calls made from ASIO.

Delayed access message services – access to stored communications

Item 12 also amends section 6 of the Act to make specific provision for the application of the definition of interception to delayed access message services. The amendments insert three new subsections into the section, and have the effect of providing that a communication sent by a delayed access message service is not passing over the telecommunications system when it is accessed in a particular way.

The amendments are intended to legislatively clarify the application of the Act to modern means of telecommunication, specifically those means of telecommunication in which there may be a delay between the initiation of the communication and its ultimate receipt by the intended recipient. The amendments do so by first defining a concept of delayed access message service in a new subsection 6(5). The subsection includes within the definition any

means by which a communication can be sent without being directly in contact with the intended recipient, and later accessed by the recipient. The definition would cover such services as fixed line and mobile voicemail services, short messaging services (SMS messaging), multi-media messaging services (MMS messaging) and email services. The definition specifically excludes voice over Internet protocol services for the avoidance of doubt.

The amendment then defines a concept of stored communication by reference to the use of a delayed access message service. Under the new subsection 6(6), a communication will be a stored communication for the purposes of the section where the communication is sent using a delayed access message service and is stored on equipment. The term will thus extend to email messages, mobile and fixed voicemail messages, SMS and MMS messaging where the relevant communication is stored on equipment. Accordingly, an SMS message stored on a mobile telephone handset, a fixed line voicemail message stored on the service provider's network and an email message saved on a recipient's home computer will all be stored communications. Messages submitted via a delayed access message service may become stored on a number of occasions and in a number of different ways during their transit between sender and recipient. New subsection 6(6) is intended to extend to all storage of telecommunications on equipment.

New subsection 6(7) specifies that a stored communication is not passing over a telecommunications system where it is accessed in particular ways. The question of when a communication is passing over a telecommunications system is central to when accessing that communication amounts to interception, requiring a telecommunications interception warrant or other appropriate exception to the prohibition against interception, and when access falls outside the meaning of interception, and may be effected by other lawful means. By specifying when communications sent by delayed access message services are not passing over a telecommunications system, the amendments clarify when the Act does not apply to these forms of communication. The amendments are intended to provide certainty in relation to the application of the Act to both users of the Australian telecommunications system whose communications are intended to be protected by the Act, and to those law enforcement and investigative bodies who may require access to communications in the course of the performance of their functions.

First, new paragraph 6(7)(a) provides that a stored communication is not passing over the telecommunications system when it is accessed by the intended recipient, or by a person with the authority of the intended recipient. The paragraph thus makes clear that such access does not amount to interception.

Second, new paragraph 6(7)(b) provides that a stored communication is not passing over the telecommunications system when it is accessed by a person other than the intended recipient after it has been accessed by the intended recipient and access is effected without using a telecommunications service or other form of remote access, except to the extent that such use is merely for the purpose of, or an incidental result of, turning on or powering up the equipment.

Finally, new paragraph 6(7)(c) provides that a stored communication is not passing over the telecommunications system when it is accessed by a person other than the intended recipient and access is effected using equipment that the intended recipient could have used to access the stored communication, whether alone or in combination with other equipment, and the access does not involve the use of a telecommunications service or other form of remote

access, except to the extent that such use is merely for the purpose of, or an incidental result of, turning on or powering up the equipment.

Both paragraph 6(7)(b) and 6(7)(c) require that access to the communication not involve the use of a telecommunications service or other form of remote access. The use of a telecommunications service includes the dialling of a number, such as dialling a voice mail box number to retrieve messages, connecting to an Internet Service Provider to access the Internet or to retrieve email, and taking advantage of or maintaining an 'always on' Internet connection for the purposes of Internet and email access. Remote access would include all forms of connectivity in which access may be achieved from a location other than that at which the data is stored. Remote access may include, but is not limited to, the use of computer network cabling or wireless connectivity via radiofrequency communications, and would extend to the use of networking connections to retrieve a communication stored on a server located elsewhere within a building, or at another location.

The paragraphs do not however preclude use of a telecommunications service or remote access where such use is merely for the purpose of, or an incidental result of, turning on equipment or obtaining power to operate the equipment. Some use of equipment used to access delayed access message services and stored communications inherently involves the use of a telecommunications service. For example, when switched on, a mobile telephone handset immediately sends out signals to locate and communicate with the nearest base station. However, for the purposes of the amendment, such use of the service provided to the handset would be an incident of turning on the equipment, rather than a user initiated communication intended to use the service provided to the handset. Similarly, the power provided to a fixed line telephone service is customarily sourced from the telecommunications line itself. However, the operation of the device through the use of power provided via a telecommunications service would be merely for the purpose of obtaining power to operate the equipment, rather than a user initiated use of the service provided to the handset, such as making a call.

The amendments therefore set out three circumstances in which stored communications are not passing over the telecommunications system, and therefore fall outside of the telecommunications interception regime and access does not require a telecommunications interception warrant. Examples of the application of the amendments to selected current technologies, and the circumstances in which a person other than the intended recipient, such as a police officer, may access stored communications pursuant to lawful authority other than a telecommunications interception warrant, are set out in the table below.

Stored communication	Application of the Interception Act and lawful access
SMS and MMS Messaging	SMS or MMS are customarily delivered directly to and stored on a mobile telephone SIM card without need for further action by the subscriber. Under paragraph 6(7)(c) a person may access those SMS and MMS messages on a mobile telephone handset using either the handset, or the SIM card in concert with a SIM card reader. Access to the messages in this manner uses equipment the intended recipient could have used (a mobile handset) or, in the case of a SIM card and reader, equipment the intended recipient could have used in combination with other equipment, and does not involve the use of a telecommunications service or remote access as it is not necessary to dial into or otherwise connect to the

network to retrieve the message – mere power to the device will be sufficient.

Fixed and Mobile Voicemail

Fixed and mobile voicemail services customarily involve the storage of the voicemail message by the service provider on its network, with the subscriber required to dial in to retrieve messages. Under paragraph 6(7)(b) a person may access voicemail messages held on a service provider's network after the communication has been accessed by the intended recipient where access is effected without using a telecommunications service. Accordingly, a law enforcement officer could not dial the voicemail box to retrieve the number, but could seek to obtain a record of the voicemail from the service provider.

Paragraph 6(7)(c) will have no application, as it would not be possible to access remotely stored voicemail messages without using a telecommunications service to initiate a communication with the service provider (such as dialling in to access the mailbox).

ISP Email

Many email services are provided through an Internet Service Provider (ISP), with users accessing their accounts through an Internet connection and an email software application. Messages may be stored at the ISP, or downloaded to the user's computer. Under paragraph 6(7)(b) a person may access email messages held on the user's home computer or the ISP's server after the communication has been accessed by the intended recipient where access is effected without using a telecommunications service. An officer could therefore obtain a copy of the message from the ISP, but could not connect to the ISP to access the account directly.

Under paragraph 6(7)(c) a person may also access those email messages on a computer that are accessible without using a telecommunications system. An officer could therefore access all messages stored on a computer that do not involve dialling into an ISP, or taking advantage of an 'always on' Internet connection.

Web-based Email

Web based email services are hosted on the Internet, with users able to access their account through any Internet connection. Messages customarily remain with the mail host, stored on the provider's equipment. Under paragraph 6(7)(b) a person may access email messages held on a service provider's network after the communication has been accessed by the intended recipient where access is effected without using a telecommunications service. Accordingly, a law enforcement officer could not connect to the Internet to access the account directly, but could seek to obtain a copy of the message from the web mail provider.

Paragraph 6(7)(c) will have no application to accessing web based email, as messages sent to a web-based email account customarily remain with the mail host, stored on the provider's computer server, unless a user takes specific action to store or copy those communications to another destination. It will therefore not be possible to access those communications without using a telecommunications service to connect to the Internet and access the account.

This item also amends the heading to section 6DA by removing the incorrect reference to 'for the use of listening devices'. The amendment corrects an earlier drafting error.

Item 11

This item inserts into the Act a transitional provision that is necessary because of the changes to the definition of interception effected by item 5. The transitional provision applies to pre-commencement warrants, that is, those telecommunications interception warrants that were issued under the Act prior to, but remain in force at, the time of the commencement of this item. The effect of the transitional provision is that pre-commencement warrants will be taken to authorise interceptions by way of reading and viewing of communications on and from the date of commencement of this item. The transitional provision will not have an adverse effect on any person.

Item 12

This item amends paragraph 15(1A)(b) to insert 'and' at the end of the paragraph. The amendment is consequential upon the insertion of a new paragraph 15(1A)(ba) into subsection 15(1A) by item 13.

Item 13

This item amends subsection 15(1A) to insert a new paragraph 15(1A)(ba). New paragraph (ba) inserts a reference to circumstances where the execution of a telecommunications interception warrant issued to ASIO will involve the taking of action by a telecommunications carrier or its employees.

Subsection 15(1A) imposes an obligation on the Director-General of Security to cause the Managing Director of a carrier to be informed of the issue of a telecommunications interception warrant to the Organisation by the Attorney-General and to be provided with a certified copy of the warrant. The inclusion of paragraph (ba) has the effect of limiting the requirement to notify the Managing Director and to provide a copy of the warrant to cases where the execution of the warrant will involve the taking of action by the carrier or its employees. The requirement to notify a carrier of the issue of a warrant by the Attorney-General, and to provide a copy of that warrant, is unnecessary in cases where effecting interception will not require action on the part of the carrier. The amendment therefore removes the requirement to notify in those cases.

Item 14

This item amends paragraph 15(4)(b) to insert 'and' at the end of the paragraph. The amendment is consequential upon the insertion of a new paragraph 15(4)(ba) into subsection 15(4) by item 15.

Item 15

This item amends subsection 15(4) to insert a new paragraph 15(4)(ba). New paragraph (ba) inserts a reference to circumstances where the execution of a telecommunications interception warrant issued by the Director-General of Security in an emergency will involve the taking of action by a telecommunications carrier or its employees.

Subsection 15(4) imposes an obligation on the Director-General of Security to cause the Managing Director of a carrier to be informed of the issue of a telecommunications interception warrant to the Organisation by the Director-General of Security in an emergency and to be provided with a certified copy of the warrant. The inclusion of paragraph (ba) has the effect of limiting the requirement to notify the Managing Director and to provide a copy of the warrant to cases where the execution of the warrant will involve the taking of action by the carrier or its employees. The requirement to notify a carrier of the issue of a warrant by the Director-General, and to provide a copy of that warrant, is unnecessary in cases where effecting interception will not require action on the part of the carrier. The amendment therefore removes the requirement to notify in those cases.

Item 16

This item amends subsection 55(5) to remove the reference to subsection (1). The reference to subsection 55(1) is no longer required as that subsection was repealed by the *Telecommunications (Interception) Amendment Act 2000*.

Item 17

This item amends paragraph 60(5)(b) to insert a reference to a certifying officer of an agency. The effect of the amendment will be to allow a certifying officer of an agency to form the view that the interception of communications to or from a particular service pursuant to a named person warrant is no longer required.

The amendment therefore extends the persons within an agency who may determine that interception of a particular service is no longer required to include certifying officers. The effect of the amendment will be to expedite the cessation of interception where interception is no longer required, and is consistent with the fact that certifying officers, by delegation from the chief officer, may revoke a service warrant where interception is no longer required.

Item 18

This item amends subsection 60(5)(b) to add a reference to a certifying officer of an agency. The amendment is consequential upon the insertion of a reference to a certifying officer in paragraph 60(5)(b) by item 17, and will allow a certifying officer to cause the Managing Director of the relevant carrier to be notified of the certifying officer's satisfaction that interception of communications to or from a particular service are no longer required.