2002-2003-2004

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT (STORED COMMUNICATIONS) BILL 2004

EXPLANATORY MEMORANDUM

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

TELECOMMUNICATIONS (INTERCEPTION) AMENDMENT (STORED COMMUNICATIONS) BILL 2004

OUTLINE

This Bill amends the *Telecommunications (Interception) Act 1979* (the Interception Act) to change the way in which the Interception Act applies to stored communications. The measures in the Bill will exclude interception of stored communications from the prohibition against interception. The amendments will have the effect of limiting the prohibition against interception to the "live" or "real time" interception of communications transiting a telecommunications system.

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 Act commences. The Act will commence on the day after the day on which it receives the Royal Assent.

Clause 3: Schedules

Clause 3 provides that each Act specified in a schedule to the Bill is amended or repealed as set out in the schedule concerned.

Schedule 1—Amendment of the *Telecommunications (Interception) Act 1979*

Item 1

This item amends subsection 6E(1) of the Interception Act to replace the existing reference to subsection 6E(2) with a reference to subsections 6E(2) and 6E(3). This amendment is consequential on the insertion of subsection 6E(3) by item 2.

Item 2

This item amends the Interception Act by inserting a new subsection 6E(3). New subsection 6E(3) excludes information obtained by intercepting a stored communication in accordance with paragraph 7(2)(ad) from the definition of the term "lawfully obtained information".

The effect of the amendment is to exclude those communications that have been intercepted in accordance with paragraph 7(2)(ad), inserted by item 3, from the restrictions on use and disclosure of intercepted material set out in Part VII of the Interception Act.

Item 3

This item amends the Interception Act by inserting a new paragraph 7(2)(ad). Subsection 7(2)(ad) provides an additional exception to the prohibition against interception set out in subsection 7(1). The amendment provides that the prohibition does not apply to or in relation to the interception of a stored communication. The term "stored communication" is defined in a new subsection 7(3A) inserted by item 4. The exception will have effect for a period of 12 months from the date of commencement of item 3.

The practical effect of the new provisions inserted by items 3 and 4 is that it will no longer be necessary to obtain a telecommunications interception warrant, or to rely on another exception to the prohibition against interception, in order to intercept a stored communication. The amendments allow for a stored communication to be intercepted by a person having lawful access to the communication or the equipment on which it is stored. A person may have lawful access to a communication, for example, with the consent of the intended recipient. A person may have lawful access to storage equipment, for example, under a search warrant or in the person's capacity as a network owner or administrator.

A telecommunications interception warrant will continue to be required in order to carry out "live" or "real-time" interceptions of communications that are in transit over a telecommunications system when intercepted. A telecommunications interception warrant will continue to be required, for example, to intercept telephone calls, facsimile transmissions and internet chat sessions and any other communication that does not fall within the definition of "stored communication" in subsection 7(3A) inserted by item 4.

Item 4

This item amends section 7 of the Interception Act to insert a new subsection 7(3A). New subsection 7(3A) defines the term "stored communication" for the purposes of new paragraph 7(2)(ad), inserted by item 3.

The definition provides that a communication will be a stored communication for the purposes of paragraph 7(2)(ad) where it is stored on equipment or any other thing. For the purposes of the definition, it does not matter whether the communication is stored prior to being transmitted, after having been transmitted or at any point in transmission over a telecommunications system.

Subsection 7(3A) further provides that the definition of stored communication does not include a voice over internet protocol (VOIP) communication held in storage on a highly transitory basis and as an integral function of the technology used in carrying the communication. VOIP is a form of packet switched data communication that involves converting audible sound into data packets for transmission over a telecommunications system. It is necessary to specifically exclude VOIP communications stored in this way from the definition of stored communication because VOIP data packets may be stored for very short periods of time while the communication is in transit. This storage is highly transitory in nature, typically lasting for only a fraction of a second and not giving rise to the creation of a permanent or retrievable copy of the communication. VOIP communications are in all other respects analogous to voice communications carried by way of standard telephony. Subsection 7(3A) ensures that a telecommunications interception warrant will be required in order to carry out "live" interception of communications carried by VOIP, and that VOIP communications are protected in the same manner as standard telephony. A voice mail message received over a VOIP service will be a stored communication, because it is held in storage on equipment and the storage is neither transitory in nature nor an integral function of VOIP technology.

New subsection 7(3A) also provides that the definition of stored communication does not include any other communication held in storage on a highly transitory basis and as an integral function of the technology used in transmitting the communication. This further exception to the definition of stored communication is necessary because other types of telecommunication, whether packet switched or circuit switched, are sometimes held in storage for very short periods of time as an integral part of the technology transmitting the communication. A short message service (SMS) or multi-media message service (MMS) communication over a mobile telephone network is an example of a circuit switched communication that may be momentarily queued or buffered as a result of network congestion. Subsection 7(3A) ensures that a telecommunications interception warrant will be required in order to carry out "live" or "real-time" interceptions of SMS messages in transit between mobile telephone users, despite the fact that the messages may be temporarily stored in transit as an integral part of SMS technology.

The following table describes the way in which the definition of stored communication in subsection 7(3A) applies to some widely used telecommunications services:

Stored communication	Application of the Interception Act and lawful access
Voice telephony	Telephone conversations over circuit switched services (eg standard telephony, GSM/CDMA mobile telephony) or packet switched services (eg VOIP, push-to-talk) do not fall within the definition of stored communication in subsection 7(3A). A telecommunications interception warrant will continue to be required in order to carry out "live" interceptions of voice telephony.
Non-voice data communications	A telecommunications interception warrant will continue to be required in order to carry out "live" interceptions of data communications (eg web content over GPRS/1xRTT). Once the data is stored (eg on a mobile telephone handset or SIM card), the definition of stored communication applies because the storage is no longer transitory in nature.
Voice mail	A voice mail message falls within the definition of stored communication in subsection 7(3A) from the time the message is deposited. A telecommunications interception warrant will not be required in order to intercept deposited voice mail messages. Rather, it will be necessary for the person seeking to intercept the voice mail to have lawful access to the message (eg with the consent of the intended recipient) or the equipment on which the message is stored (eg under the authority of a search warrant or in the person's capacity as a network owner or administrator). A telecommunications interception warrant will continue to be required in order to carry out "live" interceptions of voice telephony, which includes intercepting a telephone call in which a person is depositing a voice mail message.
SMS and MMS messaging	The definition of stored communication in subsection 7(3A) applies to SMS and MMS messages stored on a mobile telephone handset or SIM card. SMS and MMS messages stored at the premises of a telecommunications carrier or carriage service are also stored communications, provided storage is not merely transitory in nature and an integral function of the transmission of the message. A telecommunications interception warrant will not be required to intercept stored SMS or MMS messages. Rather, it will be necessary for the person seeking to intercept the SMS or MMS message to have lawful access to the message (eg with the consent of the intended recipient) or the equipment on which the message is stored

Stored communication	Application of the Interception Act and lawful access
	(eg under the authority of a search warrant or in the person's capacity as a network owner or administrator). A telecommunications interception warrant will continue to be required in order to carry out "live" interceptions of SMS and MMS messages transiting a telecommunications system.
E-mail	The definition of stored communication in subsection 7(3A) applies to stored e-mail messages. A telecommunications interception warrant will not be required to intercept stored e-mail. Rather, it will be necessary for the person seeking to intercept the e-mail to have lawful access to the message (eg with the consent of the intended recipient) or the equipment on which the e-mail is stored (eg under the authority of a search warrant or in the person's capacity as a network owner or administrator). A telecommunications interception warrant will continue to be required in order to carry out "live" interceptions of e-mail transiting a telecommunications system. This is because an e-mail is not a stored communication for the purpose of subsection 7(3A) while it is in transit over a telecommunications system. Any storage that occurs while the e-mail is in transit that is highly transitory in nature (eg momentary storage in a router in order to resolve a path for further transmission, or other buffering) and an integral function of the technology transmitting the message will not be sufficient for the communication to amount to a stored communication. However, where storage occurs that is not transitory and integral to the passage of the communication, the communication will amount to a stored communication for the purposes of the exclusion from the prohibition against interception.