Australian Government
Attorney-General's Department

Information and
Security Law Division

04/1990

12 March 2004

Senator Marise Payne
Chair
Senate Legal and Constitutional
Legislation Committee
Parliament House
CANBERRA ACT 2600

By E-mail legcon.sen@aph.gov.au

Dear Senator Payne

Inquiry into the Telecommunications (Interception) Bill 2004

I refer to the Senate's referral of the provisions of the above Bill to the Senate Legal and Constitutional Legislation Committee for inquiry on 3 March 2003, and the Committee's subsequent request for both a submission and practical examples from this Department.

The Attorney-General's Department is pleased to provide the attached submission on the Bill. Representatives of this Department would be pleased to give evidence before the Committee if this would assist in the Committee's further consideration of the proposed amendments.

The action officer for this matter is Anna Tearne who can be contacted on 6250 5422.

Yours sincerely

Peter Ford
First Assistant Secretary
Information and Security Law Division

Telephone: 6250 5425
Facsimile: 6250 5985
E-mail: peter.ford@ag.gov.au

Telecommunications (Interception) Amendment Bill 2004

Submission to Senate Legal and Constitutional Legislation Committee

General Comments

The Telecommunications (Interception) Amendment Bill 2004 amends the *Telecommunications (Interception) Act 1979* (the Act). That Act generally prohibits the listening to or recording of communications in their passage over the telecommunications system without the knowledge of the parties to the communication. That prohibition is subject to limited exceptions, including interception effected under a warrant issued under the scheme set out in the Act.

The amendments contained in the Bill are intended to ensure that the Act keeps pace with both technological developments and allows law enforcement and security agencies to effectively investigate serious criminal offences and threats to national security. The Bill addresses a number of specific issues arising in the context of telecommunications interception. These include the protection of text based communications, clarification of the scope of the protections conferred by the Act in relation to delayed communications, extension to the range of offences for which interception warrants may be sought, and the recording of calls to ASIO public lines. The Bill also amends administrative requirements in relation to the notification provided to carriers regarding ASIO warrants and the cessation of interception by law enforcement agencies.

Importantly, the Bill does not extend broader powers in relation to access to e-mail and short message service (SMS) communications. The amendments in fact more clearly protect text and image based communications, such as e-mail and SMS, and clarify how the Act applies to those telecommunications where there is a delay between sending and final receipt of a message. The Act already regulates access to all forms of communication passing over the telecommunications system. The amendments clarify the operation of the Act in this regard.

The amendments more clearly protect text and image based communications, such as e-mail and SMS, by extending the existing prohibition against interception to include reading or viewing a communication. Currently, interception is limited to listening to or recording communications in their passage over the telecommunications system.

The Bill also makes clear when access to e-mail, SMS and similar communications are protected by the Act, and when another form of access will be appropriate, such as a search warrant.
The Act currently prohibits access to communications while in their passage over the telecommunications system. The amendments specify circumstances in which a communication of this type is taken not to be passing over the telecommunications system. The amendments thus clarify what form of lawful access is required to access communications at particular points, rather than creating a new power of access.

Additional comments on the amendments contained in the Bill, including a discussion of the practical effect of those amendments, are set out below.

Protection of text and image-based communications

The Act currently provides, in section 6, that "interception" consists of listening to or recording a communication in its passage over the telecommunications system without the knowledge of the person making the communication.

The Bill amends the Act to include in the definition of interception the act of reading or viewing a communication in its passage over the telecommunications system without the knowledge of the person making the communication.

Recent developments in telecommunications technology have led to changes in the way people communicate using the telecommunications system. In particular, it is now possible to read or view, as well as listen to, a communication passing over a telecommunications system. The current definition of interception, which is limited to acts of listening and recording, does not recognise this. The definition of interception requires amendment to ensure that the Act extends appropriate protection to text and image based communications. The rapid advances in telecommunications technology of recent times are likely to continue into the future, with the use of text-based telecommunications services, such as e-mail and short message service (SMS) messages, becoming more widespread. Multi-media messaging services (MMS) are now also widely available, and are able to send high quality images via the mobile telecommunications network.

The fact that the definition of interception does not extend to reading and viewing undermines the primary object of the Act, which is to protect the privacy of individuals using the Australian telecommunications system. While listening to a voice call during its passage over the telecommunications system without the knowledge of all parties to the call is prima facie prohibited, the analogous act of reading an e-mail while in its passage is not. Thus, in cases where an email has not previously been downloaded, the Act in its present form does not prevent a person from monitoring that e-mail message, provided that the monitoring did not result in the creation of a retrievable copy of the message. Similar considerations apply in relation to SMS messages conveyed on mobile telecommunications networks, and images conveyed by e-mail or MMS.

Delayed access message services

Subject to limited exceptions, the Act prohibits listening to or recording a communication in its passage over the telecommunications system without the knowledge of the person making the communication. In its current form, the Act does not explicitly address the question of when a communication has ceased its passage over the telecommunications system, and therefore falls outside the protection of the Act.

While it is possible to determine when a standard voice communication is passing over the telecommunications system, and access is therefore prohibited subject to limited exceptions, it is more difficult to apply this test to e-mail, SMS, MMS and voicemail communications.

Recent advances in telecommunications technology have resulted in significant changes to the ways in which it is possible to communicate using the telecommunications system. In particular, a variety of delayed access message services, in which there may be a delay between the initiation of the communication and its ultimate receipt by the intended recipient, are in widespread use in the Australian community. E-mail and SMS are examples of delayed access message services.

The concept of a communication passing over a telecommunications system, while readily applicable to standard voice communications, cannot be so easily applied to delayed access message services. For instance, the application of the Act to e-mail communications is uncertain, due to the fact that it is not currently clear on the face of the legislation precisely when an e-mail message may be said to have ceased its passage over a telecommunications system. This is a relevant consideration in determining whether it is necessary to obtain a telecommunications interception warrant in order to access the communication, or whether it is appropriate to rely on some other form of lawful access such as a search warrant. Greater clarity on the face of the Act in relation to its scope will assist both law enforcement and investigative agencies to determine with certainty the appropriate form of lawful access, and will also make clear to users of the Australian telecommunications system the manner in which communications are protected and may be accessed in specified circumstances.

The Bill therefore includes amendments to make clear when access to e-mail, SMS and similar communications are protected by the Act, and when another form of access will be appropriate, such as a search warrant. The amendments do not exclude e-mail communications from the protection of the Act, but rather make clear how the Act applies to those communications.

The Bill clarifies how the Act applies to those forms of telecommunication in which there may be a delay, and transitory storage of the message, between its initiation by the sender and access by the intended recipient. These include e-mail, SMS, MMS and voicemail services. The amendments do so by specifying circumstances in which a communication of this type is taken not to be passing over the telecommunications system.

The amendments provide that a communication has ceased its passage over the telecommunications system where the communication has been accessed by the intended recipient, and access by another person (such as a law enforcement officer) does not involve the use of a telecommunications service or other form of remote access. The amendments also provide that a communication has ceased its passage over the telecommunications system where access is effected by equipment that the intended recipient could have used to access the communication, and does not involve the use of a telecommunications service or remote access.

The effect of these provisions is to exclude the act of accessing stored communications from the definition of interception when access to the communication is achieved in the manner specified. Where a communication is accessed in the manner outlined in the amendments, access to the communication will not require a telecommunications interception warrant, as such access does not amount to interception. Rather, another applicable form of lawful access, such as a search warrant, will be required in order to obtain lawful access to the stored communication.

The Explanatory Memorandum to the Bill provides some general examples of the application of the amendments to selected current technologies. Selected additional examples, focussed instead on specific hypothetical scenarios, are set out below.

Example - Home computer and e-mail

A significant number of home computer users subscribe to an account with an Internet Service Provider (ISP), providing Internet access, and usually an ISP e-mail account – for example, john.smith@isp.com.au. The Act currently enables a law enforcement agency to obtain a telecommunications interception warrant in respect of that account, provided relevant thresholds as to the seriousness of the offence under investigation and other matters are met. Accordingly, it is currently possible for intercepting agencies to access communications to and from that account in

connection with the investigation of an offence. Such access would be pursuant to an interception warrant, and effected under the scheme set out in the Act, including facilitation by the service provider.

However, a law enforcement agency investigating John Smith may instead, for a variety of reasons, seek to search Mr Smith's home. A search of the premises would ordinarily extend to computer equipment located on the premises. The computer may hold a number of e-mail messages on the computer hard disk itself. Alternatively, or in addition, there may be e-mail communications addressed to Mr Smith and held by his ISP. Mr Smith may have previously accessed some of those communications, and they are stored at the ISP on his behalf. Others may be stored unread at his ISP awaiting his next connection.

In this case, certainty as to the application of the Act is required in order to determine whether access to any or all of those communications may be obtained under a search warrant, or whether an interception warrant is required.

The effect of the amendments is that the law enforcement agency will be able to obtain access to those e-mail messages physically stored on the computer hard disk – the law enforcement officer is able to access those communications using equipment the intended recipient could have used (his home computer) and without using a telecommunications line or remote connectivity, because the computer does not need to use a telecommunications line or network cable to access those communications stored on its own hard drive.

However, in the case of the e-mail messages stored at the ISP, it will clearly not be possible for the law enforcement agency to access those communications using equipment the intended recipient could have used (a home computer or similar) without using a telecommunications line. Accessing the messages via the home computer or other equipment that Mr Smith could have used would require dialling in to the ISP. Any access not involving a telecommunications line or remote connectivity would necessarily be at the ISP's premises for storing the communication, and Mr Smith could not ordinarily have physically entered the ISP himself to extract his e-mail.

Accordingly, under the amendments proposed, access will only be possible without an interception warrant in circumstances where the intended recipient has accessed the communications, and those communications are obtained without using a telecommunications line or remote connectivity. A law enforcement agency could therefore seek to obtain e-mail communications that have already been accessed from the ISP directly pursuant to a search warrant, but could not dial in to collect those communications. Communications that have not been accessed, including those that remain in transit at the ISP, will continue to be protected by the telecommunications interception regime, and access will require a telecommunications interception warrant.

Example – SMS Messages

Mobile telecommunications networks have for some time offered Short Messaging Service, known as SMS or text messaging. The service enables mobile telephone service subscribers to send and receive short text based messages from their mobile telephone handset. Such messages are communications within the meaning of the Act, and are delivered by the telecommunications system. SMS messages are therefore prima facie protected by the Act. They may also be accessed through warranted interception of the relevant mobile telecommunications service in circumstances where the statutory prerequisites for the issue of a warrant are met.

However, while SMS messages pass over the telecommunications system and are protected by the Act during their passage, those communications are ultimately delivered to a mobile telephone SIM card. The SIM card is a Subscriber Identity Module used in a mobile telephone handset to identify the user. Text messages are automatically delivered to that SIM by the mobile service provider when the service is active – that is, when the handset is switched on.

In much the same way as a law enforcement agency may obtain lawful access to a computer, an agency may similarly obtain lawful access to a mobile handset. In these circumstances it is important that the legislation provide clear guidance on the form of lawful authority required to access any SMS messages stored on the SIM card, whether those have been viewed and retained, or not yet viewed. Similarly, there may be cases in which law enforcement requires access to SMS messages in an investigation, but does not have access to the handset or SIM card – this might, for example, be the case in a suspected kidnapping.

The amendments in the Bill provide a set of rules that assist in determining whether the relevant messages are no longer passing over the telecommunications system, and may be accessed under a search warrant or other form of lawful access, or whether those messages remain in their passage over the telecommunications system, and may only be accessed pursuant to an interception warrant.

The effect of the amendments is that the law enforcement agency will be able to obtain access to those text messages physically stored on a SIM card to which the agency has lawful access – the law enforcement officer is able to access those communications using equipment the intended recipient could have used (the SIM card, combined with either the subscriber's or another handset) and without using a telecommunications line or remote connectivity, because the SIM card does not need to use the mobile telecommunications service subscribed to to access the message, except to the extent that the device must be turned on.

In cases where the law enforcement agency does not have access to the SIM card on which the message is stored, it will clearly not be possible for the law enforcement agency to access those communications using equipment the intended recipient could have used (the SIM card). Accordingly, under the amendments proposed, access will only be possible without an interception warrant in circumstances where the intended recipient has accessed the communications, and those communications are obtained without using a telecommunications line or remote connectivity. A law enforcement agency could therefore seek to obtain SMS messages that have already been accessed from the mobile service provider directly pursuant to a search warrant. Communications that have not yet been pushed down to the handset, for example because it has not been switched on, will continue to be protected by the telecommunications interception regime, and access will require a telecommunications interception warrant.

Previous consideration by the Committee

The amendments now under consideration address a number of the issues considered by the Committee when it reviewed similar amendments introduced into Parliament in 2002 as part of the Telecommunications Interception Legislation Amendment Bill 2002. At that time, the Committee recommended that the issue of access to stored communications be considered further by the Government with a view to developing a revised approach.

The Committee received a number of submissions expressing concern that the amendments would allow access to communications without the need for a telecommunications interception warrant. The amendments do not confer wider access to e-mail and similar communications than is currently

the case, and in particular do not have the effect of permitting access to communications without an appropriate form of lawful authority.

Agencies will still require a telecommunications interception warrant to access communications that are passing over the telecommunications system. In order to access communications that are no longer passing over the telecommunications system, agencies will need to rely on some other form of lawful access, such as a search warrant.

A particular example raised by witnesses during hearings on the 2002 amendments was that of e-mail communications temporarily stored at an Internet Service Provider, and which had not yet been retrieved by the intended recipient. The amendments now proposed will ensure that a telecommunications interception warrant is required to access e-mail stored at the premises of an internet service provider where the e-mail has not previously been accessed by the intended recipient. That is, under the amendments now proposed, it will not be possible for a law enforcement agency to access an e-mail communication when it is stored at an intermediate point in transit, such as an ISP, in circumstances where that communication has not been accessed by the intended recipient.

The amendments also address concerns in relation to potential ambiguity by specifically excluding voice over internet protocol, or VOIP, services from the definition of delayed access message service. Voice services delivered over internet protocol may involve a delay, albeit a fraction of a second, in the transmission of the IP packets containing the voice message. An express provision excluding VOIP services from the application of the amendments ensures that these communications are treated in the same way as standard voice telephony.

Extension to warrantable offences

Telecommunications interception is an intrusive investigative tool. The Act protects the privacy of Australians by prohibiting the recording of or listening to communications which pass over a telecommunications system without the knowledge of the parties to that communication, subject to limited exceptions. In particular, the Act provides for telecommunications interception to be undertaken in accordance with a warrant issued under the Act. Telecommunications interception has proven to be a valuable tool in investigating serious criminal offences, and has been instrumental in securing successful prosecutions of the offenders.

The protection of privacy is balanced against the need of law enforcement agencies to access private communications in the investigation of criminal offences. The Act maintains this important balance by making telecommunications interception available only with respect to the most serious criminal offences. The Bill includes amendments to the Act to allow intercepting law enforcement agencies to apply for telecommunications interception warrants to assist in the investigation of additional terrorism offences, dealings in firearms involving planning and organisation, and State cybercrime offences.

Terrorism offences

The Bill amends the Act to allow law enforcement agencies to obtain telecommunications interception warrants to assist in the investigation of all terrorist and terrorism-related offences in the Commonwealth *Criminal Code* (the Code).

Division 72 of the 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 Code, thus ensuring the availability of telecommunications interception in connection with the investigation of those terrorism offences. This amendment supplements existing provision in the Act allowing a telecommunications interception warrant to be sought in connection with the investigation of offences involving an act or acts of terrorism.

All terrorism related offences, whether involving an overt act of terrorism or not, are extremely serious, and attract significant penalties ranging from 10 years to life imprisonment. It is therefore important that law enforcement agencies investigating terrorist and terrorism-related offences are able to make use of telecommunications interception, which has proven to be extremely effective in the investigation of other forms of serious and organised crime.

Firearms dealing

The Act currently provides for law enforcement agencies to obtain telecommunications interception warrants to assist in the investigation of offences consisting of or involving armament dealings.

The Act in its current form presents difficulties for agencies engaged in investigating offences involving firearms. Unlike the term "firearm", which generically describes any weapon capable of propelling a projectile by means of an explosive, the term "armament" has a specific ordinary meaning encompassing weaponry, munitions or other equipment of a military nature.

Law enforcement agencies may accordingly obtain telecommunications interception warrants to assist in the investigation of firearms offences only where the facts and circumstances surrounding the offence include commercial dealings in weaponry, munitions or equipment of a military nature.

The Bill therefore amends the Act to allow law enforcement agencies to obtain telecommunications interception warrants to assist in the investigation of offences consisting of or involving dealings in firearms. In order to obtain a warrant under the Act, the firearms dealings offence being investigated must also satisfy the other "planning and organisation" conduct elements set out in subsection 5D(3) of the Act. It must carry a maximum penalty of at least seven years imprisonment, involve two or more offenders and substantial planning and organisation, involve or be of a kind that ordinarily involves the use of sophisticated methods and techniques, and be committed or be of a kind that is ordinarily committed in conjunction with other offences of a like kind.

Dealings in firearms represent serious offences, and the proliferation of firearms in the community, whether military in nature or not, presents a serious risk to public safety. The Bill therefore amends the Act to enable intercepting law enforcement agencies to obtain warrants in connection with the investigation of dealings in firearms, where certain preconditions surrounding the commission of the offence are satisfied. It also avoids the anomalous result that dealings in those firearms with a

military application would be capable of enlivening the power to request a warrant, but dealings in other firearms would not.

State and Territory cybercrime offences

The Bill amends the Act to include in the definition of class 2 offence in section 5D references to State offences equivalent to those in Part 10.7 of the *Criminal Code*, thereby allowing intercepting agencies to obtain interception warrants in connection with the investigation of those offences.

The Act was amended in 1993 to include in the definition of class 2 offence the computer-related offences set out in Part VIA of the *Crimes Act 1914*. Those offences were transferred to Part 10.7 of the Code following the passage of the *Cybercrime Act 2000* and the Act was further amended in 2000 to reflect that change.

Most State jurisdictions now have in place similar legislation directed at preventing unauthorised access to, modification or impairment of computer data or electronic communications, as well as possession, control, production or supply of data with the intention of committing a computer offence.

Conduct constituting the computer-related offences in the Code and equivalent State legislation is in itself extremely serious, having the potential to severely impair the security, integrity and reliability of computer data and electronic communications. Such conduct may, in turn, lead to businesses incurring significant financial losses, compromises in the security of personal information, or damage to computer systems managing the provision of essential services. Allowing Commonwealth and State law enforcement agencies to obtain warrants under the Act to assist in the investigation of these offences is consistent with the principle of restricting access to telecommunications interception to investigations of the most serious forms of criminal activity.

Telecommunications interception also represents a particularly effective method of gathering evidence for use in the prosecution of offences involving computer data or electronic communications, and is frequently the only effective method of gathering such evidence.

Most of the existing warrantable offences in Part 10.7 of the Code and most of the equivalent State and territory offences carry maximum penalties in the range of one to 10 years imprisonment. The inclusion of these offences as warrantable offences for the purposes of the Act reflects the seriousness of the consequences of cybercrime and the fact that the best evidence for use in prosecuting these offences may be obtained by way of telecommunications interception.

Cessation of interception

Subsection 60(5) of the Act currently provides that, where the chief officer of an agency to which a named person warrant has been issued has caused the Managing Director of a carrier to be notified that a service operated by that carrier is to be intercepted under the named person warrant, and where the chief officer of that agency is satisfied that interception of the service is no longer required, the chief officer must cause the Managing Director to be informed forthwith and provide confirmation in writing to the Managing Director as soon as possible.

The Bill amends the Act to provide that, where the chief officer of an agency to which a named person warrant has been issued has caused the Managing Director of a carrier to be notified that a service operated by that carrier is to be intercepted under the named person warrant, and where the chief officer or a certifying officer of that agency is satisfied that interception of the service is no

longer required, the chief officer or the certifying officer must cause the Managing Director to be informed forthwith and provide confirmation in writing to the Managing Director as soon as possible.

In its current form, subsection 60(5) of the Act requires that, in order to cease intercepting individual telecommunications services under the authority of a named person warrant, the chief officer of the agency to which the warrant was issued must be personally satisfied that the interception of that service is no longer required. It is not consistent with the underlying policy of the Act to place such a limitation on an agency's ability to cease intercepting a telecommunications service. The need for personal satisfaction at chief officer level whenever an agency wishes to cease intercepting a telecommunications service under a named person warrant also places an unnecessary administrative burden on chief officers and their staff.

The proposed amendment to subsection 60(5) will extend to senior staff of each agency the power to certify that the interception of a particular telecommunications service is no longer required and should therefore cease. It is appropriate that, where a certifying officer is satisfied that interception of a particular telecommunications service is no longer required, that certifying officer be required to cause the Managing Director of the carrier operating the service to be advised accordingly.

The effect of the amendment will be to ensure that an interception may be ceased as soon as a certifying officer forms the view that the interception is no longer required. In this way the amendment enhances, rather than reduces, the safeguards against unwarranted interception set out in the Act.

Carrier notification

The Act currently requires that, where ASIO is issued with a warrant authorising the interception of telecommunications services, the Director-General of Security must inform, and provide a copy of the warrant to, the Managing Director of the telecommunications carriers whose service is to be intercepted under the warrant.

The requirement to inform and provide a copy of the warrant to the carrier is however not always operationally appropriate for ASIO. There are circumstances where it may not be necessary or appropriate to secure the assistance of the carrier in order to execute the warrant. This may be in cases of emergency or where notification to the carrier would be prejudicial to security. In these cases, the requirement to notify the carrier is unnecessary and adds nothing to the extensive accountability regime established under the Act.

The Bill therefore amends the Act to remove the requirement to notify the relevant carrier of the issue of a warrant in circumstances where that carrier's assistance is not required to execute the warrant. These amendments will not adversely affect protections conferred by the Act. Rather, the amendments will ensure that the requirement does not apply where ASIO does not need the carrier's assistance. ASIO will continue to require a warrant issued by the Attorney-General to intercept communications passing over the Australian telecommunications system.

Recording of ASIO public lines

The Act defines interception as the act of listening to or recording a communication in the course of its passage over the telecommunications system without the knowledge of the parties to the communication. While the Act sets out a number of exceptions to that prohibition, including interception under warrant and without warrant in specified circumstances, the Act contains no general exemption from the prohibition against interception permitting the recording of calls to publicly listed services maintained by ASIO.

The Bill amends the Act to allow ASIO to intercept calls to its public lines without advising the person making the call.

ASIO maintains a dedicated exchange line in its Central Office and each Collection Office within the States and Territories, the numbers for which are listed in public telephone directories. It also maintains a toll free service for general inquiries. ASIO public lines are used by members of the public to contact ASIO when wishing to pass on information which they consider relevant to ASIO's functions of collecting intelligence relating to national security. These numbers are vital for ASIO to receive information by telephone from members of the public. These numbers have also been used to convey threats to Australian institutions and persons.

Calls made to ASIO public lines provide an important source of information, accurate records of which are instrumental in ensuring that ASIO is able to respond quickly and effectively. The inability of ASIO to accurately monitor or record calls to ASIO public lines is an operational issue which may hinder the effective investigation of matters of national security.

Calls to ASIO public lines may involve information that needs to be acted on urgently and the time taken to advise each caller represents an unacceptable delay. An express notification may also deter callers from contacting the public lines to provide tip-offs or other information relevant to security.

The amendments therefore ensure that calls to ASIO public numbers, potentially providing information critical to security, can be accurately recorded without the requirement to first notify the caller of the fact of the recording.