Telecommunications (Interception and Access) Amendment Bill 2009

1.1 Overview

The focus of the Telecommunications (Interception and Access) Amendment Bill 2009 (the Bill) is to amend the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to introduce a network protection regime that enables all network owners and operators to protect their network and the information it contains.

The Bill also makes a number of technical amendments to maintain the currency of the TIA Act.

1.2 Network Protection

Increased use of online services by individuals, governments, business and the not-for-profit sector means sensitive information is regularly transmitted and stored electronically. Accessing or disrupting the carriage of this information can provide significant financial and other benefits for criminal elements. Consequently, protecting information and computer infrastructure from malicious attack is a key concern both for governments and for the growing number of computer network owners whose networks hold and transmit such information.

Not all network protection activities are currently lawful under the TIA Act. Whether an activity is lawful depends on the particular characteristics of the activity that is undertaken, where it is undertaken, by whom, and whether or not there is awareness by the affected person that it is being done. For example, persons undertaking network protection activities may need to copy a communication before it is delivered to the intended recipient for filtering purposes or further inspection. However, under the TIA Act, copying is only allowed at certain points in the delivery of that communication and under certain conditions. This means that network owners and operators are vulnerable to inadvertently breaching the law prohibiting interception.

The TIA Act currently includes special exemptions that enable interception and security agencies, as well as certain Government Departments, to access communications on their own computer network for network protection activities.

These provisions were originally introduced by the *Telecommunications (Interception) Amendment Act 2006* in order to allow the Australian Federal Police (AFP) to protect its network and to ensure staff were complying with the AFP's professional standards. At the time, Parliament legislated a two year sunset period for the provisions in order to allow consideration of a more comprehensive solution.

In 2007, the provisions were widened to the current form to allow government agencies and authorities with a security or law enforcement focus to monitor communications for the purpose of protecting their networks and enforcing professional standards without the risk of breaching the TIA Act. At the time the Senate Standing Committee on Legal and Constitutional Affairs noted that the provisions protected these agencies on an interim basis while a permanent solution applicable to both the public and private sectors, which takes into account developing technologies and threats, systems administration procedures and workplace privacy, was being developed.

In 2008, Parliament extended the sunset clause until the end of 12 December 2009 in order to allow broader consultation with the non-government sector on a network protection solution. In its report on the 2008 Amendment Bill, the Senate Standing Committee on Legal and Constitutional Affairs

noted that "further legislation proposing amendments to the network protection provisions…should include a thorough and considered response to achieving a balance between individual privacy rights and network protection requirements. Such a review should assess mechanisms to mitigate intrusiveness and abuse of access, and consider how secondary data may be managed appropriately."

Development of network protection regime proposed in the 2009 Bill

Consistent with these concerns, the Bill delivers a system that enables all Australian network operators and owners to undertake activities to operate, maintain and protect their networks while protecting users from unnecessary or unwarranted intrusion.

Following ongoing internal consultation with key stakeholders from both the government and non-government sectors, draft legislation detailing a possible approach to network protection was prepared for public consideration.

The exposure draft was released on 17 July 2009 together with a comprehensive discussion paper that detailed the current system and the proposed legislative approach set out in the draft Bill. Correspondents were asked to provide their comments by 7 August 2009 in order to allow legislation to be introduced and debated in Parliament prior to the expiry of the current network protection provisions at the end of 12 December 2009.

Public exposure draft Bill and Discussion Paper

The exposure draft legislation proposed a voluntary, technology neutral system that maintained the existing privacy threshold within the TIA Act by maintaining the prohibition against interception for network protection purposes, unless the interception complies with certain specified conditions.

These conditions are that such interceptions must be carried out by a person lawfully engaged in duties relating to the protection, operation or maintenance of the network or ensuring its appropriate use, and that the interception is reasonably necessary for the performance of those duties.

Importantly, the draft Bill specified that the proposed network protection regime would operate within the general framework of the TIA Act including the existing limitations on the secondary use and disclosure of lawfully intercepted information set out in Part 2-6 of the Act. This meant for instance, that network operators could not be compelled to provide information obtained through network protection activities (including information disclosing criminal or illegal behaviour) nor would it be lawful for law enforcement or security agencies to request such information. Rather, the draft Bill allowed information to be used or communicated on a discretionary basis where it was reasonably necessary to do so for the purpose of protecting the network, or to respond to an inappropriate use of the network.

Under the draft Bill network operators and owners could also undertake network protection activities to ensure their network was being used appropriately by employees and to use or communicate related information for network protection purposes. This information could also be used or communicated to others for disciplinary purposes in relation to an employee where a user agreement outlining the conditions of appropriate use was in place between the employee and the owner or operator of the computer network. Information could not be used for disciplinary purposes in the absence of a user agreement.

This capability reflected the existing capacity of government agencies covered by the current network protection provisions and recognised the need to protect public and private networks and information from internal misuse or attack.

Amendments resulting from stakeholder consultation

The exposure draft Bill and discussion paper were made available on the Departmental website. All known stakeholders who have expressed previous interest in network protection were contacted directly and over 700 subscribers to the Office of the Privacy Commissioner's electronic newsletter were advised of the consultation in that newsletter.

The Department received 19 substantive submissions. The Department has not made these submissions available publicly as the submissions may contain commercial or operationally sensitive information.

The majority of submissions supported the general approach set out in the draft Bill and discussion paper. Several issues were highlighted whose inclusion in the Bill would improve the operation of the scheme and the Bill was amended accordingly.

The draft Bill was amended to:

- improve operational effectiveness by allowing organisations to designate more than one person or position in an organisation as being responsible for authorising network protection duties and for destroying network protection information when no longer required;

- emphasise the voluntary nature of the network protection regime and the focus of disciplinary action on the activities of certain government employees; and to

- provide standard recordkeeping obligations across the government and non-government sectors.

The voluntary nature of the scheme was a key issue with several submissions expressing concern that a network protection regime should not compel the monitoring of users' activities. Particular concerns were expressed that the inclusion of employee activities within the scope of network protection duties was broader than was needed to protect network infrastructure and security in a regime that is not compulsory and, in the case of the non-government sector, predominantly self-regulated.

Consequently, the Bill provides that network protection activities and network protection information will only be able to be undertaken, used and communicated for disciplinary purposes by Commonwealth agencies, security authorities and eligible authorities as currently defined under the TIA Act. Use for these purposes is consistent with the current network protection provisions and reflects the fact that these agencies and authorities are subject to additional professional standards and statutory requirements not applicable to other public sector or non-government employers.

However, the Bill goes beyond the existing provisions to provide new protections for workers in the agencies and authorities covered by these provisions. Under these requirements network protection information will only be able to be communicated or used for disciplinary purposes where a user has undertaken to comply with reasonable conditions set out in a written user agreement and where

that communication or use is not prohibited by another State, Territory or Commonwealth law. Any subsequent disclosure by an individual who has received information for the purpose of disciplinary action must also accord with Commonwealth, State or Territory laws.

1.3 Other Amendments

Amendments to subsection 5(1) – New South Wales Police Integrity Commission

These are consequential amendments that update subsection 5(1) of the TIA Act to reflect the transfer of certain functions from the Independent Commission Against Corruption (ICAC) to the New South Wales Police Integrity Commission (PIC).

Amendments to the *Police Integrity Commission Act 1996* (NSW) (the PIC Act) which came into effect on 1 July 2008 mean that the role of the PIC has expanded to investigate the corrupt conduct of administrative officers of the New South Wales Police Force and misconduct of Crime Commission officers.

The proposed amendments to the TIA Act will enable the PIC to use and communicate lawfully intercepted information for the purpose of an investigation in relation to any officer within the PIC's jurisdiction.

Amendments relating to the Australian Federal Police (AFP)

The Criminal Code contains provisions that enable the AFP to apply for control or preventative detention orders in order to prevent a terrorist attack.

Control orders are protective measures that allow controls to be placed on a person's movements and activities (similar to a domestic apprehended violence order). The AFP can apply to a court for a control order where there are reasonable grounds that a control order would assist in preventing a terrorist act or that a person has trained with a listed terrorist organisation.

The preventative detention regime enables the AFP to take a person into custody and detain them for a period of 48 hours to prevent a terrorist attack occurring, or to preserve evidence of a recent terrorist attack.

The Department is of the view that the nature of the offences associated with control orders and preventative detention orders means that the AFP is authorised to use lawfully intercepted information in these applications. However, the issue has not been considered by a court and, in the absence of a specific reference, there is some risk a court could find that information obtained under the TIA Act is not available for these purposes. Any uncertainty will be removed by the amendments proposed in the Bill which specifically allow the disclosure and use of intercepted information in applications for control orders and preventative detention orders.

The Bill also includes provisions validating the communication, use or recording of such information prior to the commencement of the Bill so as to ensure the validity of information used in control order applications.

These amendments preserve the status quo and do not increase the powers and functions of law enforcement agencies under the TIA Act.

Extension of the evidentiary certificate regime and associated amendments

Currently, the TIA Act includes an evidentiary certificate regime for intercepted and stored communications. Under this regime, designated persons can issue a written certificate setting out such facts as the signatory considers relevant with respect to acts or things done by, or in relation to, employees of a carrier in order to enable an interception warrant to be executed. Such certificates can be received in evidence in certain legal proceedings without further proof and are conclusive evidence of the matters stated in the certificate.

Law enforcement agencies and ASIO can also issue such certificates in prescribed circumstances, setting out such facts considered relevant with respect to acts or things done by, or in connection with, enabling a warrant to be executed and in connection with the execution of a warrant. Such certificates are prima facie evidence of the matters stated in the certificate.

The *Telecommunications (Interception and Access) Amendment Act 2007* (the 2007 Amendment Act) transferred relevant aspects of the telecommunications data access regime from Part 13 of the Telecommunications Act to the new Chapter 4 of the TIA Act. This enacted the second tranche of the Blunn Review recommendations aimed at implementing comprehensive and over-riding legislation dealing with access to telecommunications information for security and law enforcement purposes. The provisions as transferred did not include an evidentiary certificate regime for telecommunications data.

The amendments contained in this Bill will extend the evidentiary certificate regime to include access to telecommunications data. Under the provisions, the Managing Director or secretary of a carrier, or of a body corporate of which the carrier is a subsidiary, will be able to issue a written evidentiary certificate which is conclusive evidence of the acts or things done by an employee of the carrier to enable the lawful disclosure of telecommunications data to ASIO or an enforcement agency.

The conclusive nature of carrier certificates is consistent with sections 18 and 61 of the TIA Act concerning evidentiary certificates relating to the interception of communications under warrants. Similarly, section 129 of the TIA Act, which allows carriers to issue conclusive certificates relating to the execution of stored communications warrants, was modelled on sections 18 and 61.

Like proposed section 185A, certificates made under sections 18 and 61 of the TIA Act relate to subsidiary matters of a procedural nature relevant to the execution of a telecommunications service warrant and deal with technical issues within the particular expertise of the carrier giving the certificate which would otherwise be difficult and time-consuming to prove. In the absence of a conclusive certificate, carrier employees would need to appear in court to give evidence about the actions they took to enable the execution of a warrant. This would expose the identity of individual employees and could reveal sensitive information about technological and interception capability potentially undermining the veracity of the interception regime.

While conclusive in nature and therefore not contestable, these certificates do not address nor prove the substantive elements of an offence. At the most, the certificate establishes that a carrier intercepted certain communications sent from a particular telecommunications account. The prosecution still has to prove all the elements of the offence with which the accused is charged.

In 2008, the New South Wales Criminal Court of Appeal unanimously upheld the constitutional validity of section 18 certificates (*Cheiko v Regina* [2008] NSWCCA 191) rejecting a request to appeal a decision by the trial judge, Justice Whealy, to uphold the conclusive nature of the certificates. Justice Whealy noted that Parliament had balanced competing public interests in prescribing the conclusive element and acknowledged that the purpose of the provision was to protect the identity of carrier employees engaged in the execution of interception warrants. His Honour also noted that the certificates address only formal matters of evidence and do not prove any facts in issue before the court.

The introduction of an evidentiary certificate regime for telecommunications data was delayed pending the outcome of the *Cheiko* proceedings and its inclusion in this Bill will introduce a uniform approach throughout the TIA Act.

The Bill will also allow the Managing Director or secretary of a carrier, or of a body corporate of which the carrier is a subsidiary, to delegate in writing to an employee of the carrier the ability to issue a conclusive certificate in relation to warrants issued to ASIO, stored communications warrants and the proposed evidentiary certificate regime for telecommunications data.

Delegation of this administrative function will enable people more actively involved in interception activities to issue conclusive certificates and will enable certificates to be issued in a more timely manner. Certificates are often required urgently to meet court deadlines and proceedings can be delayed if the Managing Director or Secretary is not available. Carriers have experienced difficulties in complying with the existing requirements and have requested amendments to allow this function to be delegated.