



Australian Government

Attorney-General's Department

**DISCUSSION PAPER AND EXPOSURE DRAFT
LEGISLATION**

Computer Network Protection

July 2009

Call for Public Comment

The Australian Government has approved the release of exposure draft legislation to facilitate public consultation on proposed reforms to the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) intended to improve the capacity of owners and operators of computer networks to undertake activities to protect their networks.

The rapid uptake of information and communications technology (ICT) in Australia is transforming the way we interact, do business and conduct our personal affairs. All sectors of the Australian community are becoming increasingly reliant on ICT to relay and store sensitive information.

In 2008, the Australian Bureau of Statistics (ABS) reported that between June 2006 and June 2007, 86 percent of all businesses reported that they used the internet. A third of all businesses reported they had a web presence, 40 percent of all businesses reported they had placed orders via the internet or web, and just over a fifth of all businesses reported they had received orders via the internet or web. Businesses estimated that approximately \$68 billion was generated by these orders, or 3.5 percent of total income from the sales of goods or services.¹

The ABS has reported that as of December 2008, there are almost 8 million subscribers to the internet in Australia. Of these, 1.3 million are business and government subscribers, and 6.7 million are household subscribers.² It is predicted that with the implementation of the super fast National Broadband Network, announced by the Government in April 2009, 90 percent of all Australian workplaces, schools and homes, will be connected to the internet by broadband services of speeds 100 times faster than those currently used by many businesses and households. All other premises will be connected by next generation wireless and satellite technologies delivering broadband quality speeds.³

While the uptake of ICT offers enormous potential for people to connect with others and grow businesses locally and internationally, it has also opened the door to new threats. As sectors of the community become more reliant on ICT to relay and store sensitive information, the potential grows for people, including organised crime and terrorist groups, to harm individuals and organisations through malicious access to such information. Accordingly, protecting sensitive information 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.

¹ Australian Bureau of Statistics *Selected Characteristics of Australian Business, 2006-07* (cat. no. 8167.0). Report issued 19/9/2008.

² Australian Bureau of Statistics *Internet Activity, Australia, December 2008* (cat. no. 8153.0). Report issued 6/4/2009.

³ *New National Broadband Network*. Joint Media Release by the Prime Minister, Treasurer, Minister for Finance and the Minister for Broadband, released Canberra, 7 April, 2009. Available at http://www.minister.dbcde.gov.au/media/media_releases/2009/022.

Computer networks require testing, monitoring and maintenance to ensure they are not vulnerable to known or predicted security risks and are able to repel or survive an attack. They also require such monitoring and maintenance to ensure that they operate in an efficient manner, are free of misconfigurations, and that network traffic can travel at optimal speeds.

Activities undertaken for the purpose of protecting a network are critical to both its efficient operation and the protection of all data stored on the network. Such data may include sensitive government and business data held on the network, as well as any personal and financial data which individuals have supplied, for example in the course of their employment or in requesting or purchasing services.

However, some network protection activities are unlawful under the TIA Act. Although a number of government agencies are protected by an exemption under the TIA Act, this exemption is only effective until 13 December 2009. This limited timeframe was designed to enable these agencies to undertake network protection activities while a broader solution, applicable to the general community, was developed.

The Attorney-General's Department has developed a proposal to amend the TIA Act to allow all owners and operators of computer networks in Australia to undertake activities to protect their networks. The details of the draft proposal are set out in this paper.

Several principles have guided the development of the proposal:

1. The solution must be comprehensive and flexible to accommodate all computer networks
2. The solution should be technology neutral to ensure ongoing relevance as technology advances, and
3. The solution must balance the need to protect information with the need to protect users from unnecessary or unwarranted intrusion.

This proposal has been developed in consultation with key stakeholders and is now open for public comment. In order to assist public comment, the Australian Government has approved the release of draft legislation which shows how the proposed network protection regime could be accommodated in the TIA Act. The Australian Government welcomes your comments on the proposed legislative provisions.

How do I comment?

Comments are sought by 7 August 2009 in order to allow legislation to be introduced and debated in Parliament prior to 13 December 2009.

Comments can be emailed to the Attorney-General's Department at tslb@ag.gov.au or mailed to:

Telecommunications and Surveillance Law Branch
National Security Law and Policy Division
Attorney-General's Department
3-5 National Circuit
Barton ACT 2600

NETWORK PROTECTION DISCUSSION PAPER

Computer networks rely on the efficient and secure transmission of information. Thus, networks must be monitored to ensure that network traffic operates as intended and that any misconfigurations, failures or user errors are readily identified and rectified. Networks also need to be tested to ensure that the network is not vulnerable to, or has not been subject to, an attack.

The increased use of online services by individuals, government and business means sensitive information is regularly transmitted and stored electronically. Such information includes personal information (names, addresses, associations and preferences), financially sensitive information (online banking and credit card details), commercially sensitive information, government information, and passwords/credentials used to access computer systems or networks.

Accessing this information can provide significant financial and other benefits for criminal elements and competitors and be highly costly to affected businesses. For example, it is estimated that Australian businesses lost between \$595-\$649 million in the 2006-7 financial year due to computer security incidents.⁴ As the number and sophistication of these attacks grow, we can only expect these costs to rise. Verizon Communications, an American broadband and telecommunications company, has reported a significant recent rise in the extent to which computer held records have been compromised. Verizon Communications investigated 90 confirmed cases of data breaches (being loss or compromise of data stored on or transmitted by computers) in 2008 and identified more than 285 million records that had been compromised. These compromises occurred across all sectors, including the financial, retail, and government sectors, the number of records being compromised exceeding the combined total of records compromised between 2004 and 2007.⁵

Computer attacks take many different forms, including viruses, Trojans, denial of service attacks and more sophisticated attacks. Typically, intruders enter networks by tricking a legitimate user into inadvertently running malicious code, or by exploiting weaknesses in software products used on the network. Attacks may be perpetrated by individuals, competing entities, organised crime groups or by state based entities. They may be launched from within the network, or may be conducted from within the country of operation or from overseas.

Preventing an attack from entering or proliferating within a network is critical to securing the integrity of valuable and sensitive information held in that network, and ongoing monitoring is essential to ensure the network's efficiency and resilience.

⁴ Richards, K. (2009) *The Australian Business Assessment of Computer User Security: a national survey*. Australian Institute of Criminology, Research and Public Policy Series, Report 102.

⁵ *Verizon Business: 2009 Data Breach Investigations Report* available at <http://www.verizonbusiness.com/us/resources/media/1008a1a3-111=129947-Verizon+Business+2009+Data+Breach+Investigations+Report.xml>.

What is network protection?

Network protection usually involves establishing perimeters to defend a network by placing protective tools at different points within the network to detect and respond to known and predicted security risks.

In many organisations, defensive network protection activities are supplemented by proactive steps, such as ‘hacking’ into an organisation’s own network, to identify weaknesses in the network. Once identified, weaknesses can be fixed in order to strengthen the network from possible attack.

The time between compromise of a network and detection can vary markedly, as can the time between detection and containment.⁶ The longer the time between detection and containment, the greater the chance that sensitive financial, personal and other data an organisation holds may be stolen, sold onto the black market, or used to design further attacks.

The capacity to stop or to prevent an attack is critical to protecting the integrity of stored information. As technology advances, the prevalence of sophisticated attacks is likely to increase. In turn, more complex and potentially more intrusive network protection activities can be expected. While the imperative to protect sensitive information is strong, the potential for more intrusive activities needs to be balanced against the ability of employees to maintain an appropriate level of privacy in the workplace.

While all workplaces have different operational needs and cultures, many workplaces allow employees to use the network for reasonable or acceptable personal use, much in the same way as they allow employees to make reasonable use of telephones to deal with personal matters during working hours. The concept of what amounts to acceptable personal use will vary from workplace to workplace, and is a matter for employers to negotiate with their staff.

Facilitating network protection, while enabling users to maintain an appropriate level of privacy in the workplace, is a key challenge in designing a network protection regime that is relevant to current needs and which is adaptable to future change.

What does the current network protection regime allow?

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.

⁶ For example, the *Verizon Business: 2009 Data Breach Investigations Report*, at p.35 indicates that in 2008, 8 percent of compromises took only a number of hours to be detected and 49 percent of compromises took months to be detected. Of these, 6 percent of compromises took only a number of hours to be contained from the time they were detected, 37 percent took days to be contained, and 42 percent took weeks to be contained.

For example, persons undertaking network protection activities may need to copy a communication before it is delivered to the intended recipient. Under the TIA Act, copying is only allowed at certain points in the delivery of that communication and under certain conditions.

The TIA Act defines interception as copying a communication while it is passing over the network. A communication is 'passing over the network' while it is travelling between the points where it entered the network (for example, the firewall) and where it becomes available to the recipient at the mailserver. Unless an exception is available under the Act, interception is an offence punishable by imprisonment for up to two years.

It is not interception to copy a communication once it has finished passing over the telecommunications system and has reached the recipient's mailserver. Therefore, persons undertaking network protection activities for a particular network can legally access, read, copy or delete every communication once it has reached the recipient's mailserver.

However, copying the same communication prior to its delivery is an interception if it is done without the knowledge of the person sending the communication. Under the TIA Act, copying a communication while it is passing over the telecommunications system is not interception if it takes place with the knowledge of the person making the communication.⁷

The users of most government, corporate and institutional networks agree to conditions of use as a prerequisite to using that network. The conditions commonly include provisions for a person's use of the network to be monitored for compliance with the conditions of use. Such agreements mean that network owners or operators can access all communications originating from internal users without breaching the TIA Act.

While this covers all internal internet usage and a significant proportion of email traffic, communications by internal users who have not signed a user agreement are not covered, nor are inbound communications from persons who do not have knowledge that their communications may be accessed.

The inability to access inbound communications prior to their delivery is a significant constraint on the effectiveness of network protection as most attacks stem from external sources and have the potential to do considerable damage to the network if they are not identified and addressed prior to reaching the delivery point.

The TIA Act currently includes special exemptions so that certain law enforcement and oversight agencies and certain security authorities can protect their networks irrespective of the source of that attack.⁸

Under these provisions, a communication only begins to pass over a telecommunications system once it has left the boundaries of the agency's network.⁹

⁷ Section 6 of the TIA Act.

⁸ See sections 5, 5F and 5G of the TIA Act.

In addition, agency employees or representatives responsible for operating, protecting and maintaining the network or enforcing professional standards are deemed to be 'intended recipients' of all communications addressed to a person at an address on a computer network operated by or on behalf of an agency and can lawfully access the communication.¹⁰

Together these provisions give national security and law enforcement agencies greater legal capacity to monitor and protect their networks from malicious attack. However, the provisions are not permanent. Rather, they were designed to operate on an interim basis pending the implementation of a comprehensive solution covering both the public and private sectors. These provisions expire on 13 December 2009. From that date, new provisions are needed to provide clear authority for all owners of Australian networks to undertake network protection activities prior to the point at which a communication is delivered.

What is the proposed approach?

The Australian Government considers that the TIA Act does not currently provide sufficiently clear guidance on when network protection activities can be lawfully undertaken. This leaves network owners and operators exposed to the possibility of inadvertently breaching the law prohibiting interception.

In addition, the TIA Act does not provide sufficient guidance on the legitimate use and secondary disclosure of information accessed by network owners or operators for network protection purposes. Therefore, in the absence of other relevant statutory duties, there is a real risk that information could be used inappropriately against network users. Furthermore, there is also the risk that information suggesting inappropriate or illegal conduct by an employee could not successfully be used in evidence in a disciplinary or criminal hearing.

Consequently, the proposed reforms are focused on implementing a single network protection regime that is relevant to all computer networks and their owners and operators within Australia.

One approach to network protection would be to extend the existing network protection provisions beyond those government agencies currently able to utilise them to cover all computer networks. This would mean exempting all network protection activities from the definition of interception. The Australian Government is of the view that such an approach is inconsistent with the fundamental principle underpinning the TIA Act, namely, that communications should remain private except in clear circumstances where the law provides specific direction.

Instead, the legislative approach proposed in the exposure draft attached to this paper recognises the general prohibition against interception and clearly defines the circumstances in which the access, use and disclosure of information is permitted.

⁹ See subsection 5F(2) of the TIA Act.

¹⁰ See subsection 5G(2) of the TIA Act.

Network protection

Under the proposed legislative approach, network protection activities which copy or access a communication, without the knowledge of the sender, while it is passing over a computer network will constitute an unlawful interception unless the activities meet 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 the interception is reasonably necessary for the performance of those duties.¹¹

Accordingly, a communication will be considered to be intercepted if it is copied or accessed without the knowledge of the sender:

- after it has entered a network and prior to its delivery to the intended recipient
- after it has been sent by an internal sender and not yet received by the internal intended recipient, and
- after it has been sent by an internal sender and not yet exited the computer network.

That interception will be unlawful unless it is 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 the interception is reasonably necessary for the performance of those duties.

Information that is intercepted by way of network protection activities will be subject to the general prohibition on the secondary use and disclosure of lawfully intercepted information, subject to the relevant exceptions that include:

- making records for the purpose of lawfully communicating the relevant information
- the disclosure of information between law enforcement agencies and for the purposes of national security, and
- giving evidence in certain proceedings.

In addition, if a person obtains information as a result of undertaking network protection activities, they will be able to use or communicate that information to another person if it is reasonably necessary to do so for the purpose of protecting the network, or to respond to an inappropriate use of the network.

¹¹ See clause 8 of the draft legislation.

The proposed amendments will not authorise the interception of speech for network protection purposes.¹² This means that telephone communications will not be accessible under these provisions. Voice communications travelling in packet data form, for example by way of Voice over Internet Protocol (VoIP), may be intercepted and disclosed in that format. However, any information gained by reconstituting the communication into speech may not be communicated to another person or otherwise be made use of.¹³

Appropriate use of a computer network

Although recent evidence now shows that the majority of threats to a network emanate from sources external to that network, it is still prudent for network owners and operators to ensure that employees are using the network appropriately and are not exposing the network to unnecessary threats. A network protection regime which offers strong defences against intruders trying to ‘hack’ into the network but does not prevent employees from downloading malware is unlikely to provide a strong level of protection to sensitive commercial or government data.

Accordingly, the proposed legislative provisions will enable the owners and operators of computer networks to implement measures to ensure that their computer networks are used appropriately by employees, and will allow owners and operators to use or communicate that information to others for network protection purposes.¹⁴

That information will also be able to be used or communicated to others for disciplinary purposes where a user agreement which outlines the conditions of appropriate use is in place between the user and the owner or operator of the computer network.¹⁵ If no user agreement is in place, that information will not be able to be used for disciplinary purposes.

As each organisation will have a different concept of what constitutes ‘appropriate use’ of a computer network within their organisational context, it is not proposed to comprehensively define the terms ‘appropriate use’ and ‘appropriate action’ in the TIA Act. This will enable the diversity of occupations and organisational focus of network operators and owners to be covered by the proposed network protection provisions. For instance, a small retail business is likely to have a different view on what constitutes appropriate use of its corporate network from a larger company whose business is focused on providing IT related services to clients.

Rather, the terms ‘appropriate use’ and ‘appropriate action’ will be defined by reference to the uses and actions that have been agreed in writing between individual users and the operators of specific networks.

¹² See clause 10 of the draft legislation.

¹³ See clause 11 of the draft legislation.

¹⁴ See clause 11 of the draft legislation.

¹⁵ See clauses 6 and 11 of the draft legislation.

Clause 6 of the draft legislation creates this link by stating that a computer network is ‘appropriately used’ when the user:

- (a) has given a written undertaking to use the network in accordance with any written conditions specified by the network owner or operator
- (b) complies with those conditions, and
- (c) the conditions are reasonable.

It is anticipated that most existing IT user agreements will suffice in these circumstances.

The legislation will also identify who can receive intercepted information and for what purpose. In particular, information collected for network protection purposes which is relevant to potential disciplinary action against a network user can only be communicated to another person for that purpose where no other Commonwealth, State or Territory law would prohibit such communication. This limitation protects employees by ensuring that employers cannot circumvent any relevant State or Territory workplace relations requirements by accessing information under the TIA Act.

Regulatory impact of ‘appropriate use’ provisions

There is no expected impact of the proposed appropriate use provisions in the TIA Act.

Existing user agreements will be recognised by the proposed legislation and it will be left to the discretion of each organisation as to whether or not they choose to put in place a user agreement.

In order to be effective, user agreements must be in writing, and their terms must be reasonable. However, the exact terms of user agreements will be a matter for negotiation between organisations and their employees.

If no user agreement is in place, intercepted material concerning an employee’s use of the network will not be able to be used for disciplinary purposes.

The following examples indicate how the legislation could work in practice.

New network protection provisions – Scenario 1

Peter Jones is a pharmacist who runs a pharmacy employing 10 people. While the business is small, it has a large client base. As the business holds a significant amount of personal information relating to its clients, Peter has contracted an IT security firm to protect the pharmacy’s computer network.

Under the proposed legislation, as the security firm has been contracted on behalf of Peter to provide network protection services, the firm can lawfully intercept communications on the pharmacy’s network in order to perform its network protection function.

As part of the terms of employment, all pharmacy employees must sign a network user agreement which, amongst other requirements, states that users must not access client records for any purpose unrelated to a client's health outcomes. The agreement states that email traffic may be monitored to ensure that users are not breaching the agreement and that information obtained through monitoring activities may be passed on to relevant government authorities.

Protective software identifies a number of emails which indicate that identifying client details have been accessed by an external party. Further investigation suggests that a pharmacy employee is involved in the unauthorised provision of information and several incoming emails intercepted recently at the firewall reveal that a further exchange of information is due to take place soon.

Under the proposed amendments to the TIA Act, the security firm would be able to notify Peter as the pharmacy head that the computer network has been accessed by a third party. As Peter is responsible for employment and disciplinary actions within the pharmacy and, in this case, no relevant State workplace surveillance laws apply, the security provider would also be able to provide details to Peter about the communications sent by the employee suspected of supplying the information.

Peter is notified and suspects, based on the nature of the information affected, that criminal activity is involved. Provisions in the planned amendments will allow Peter to communicate the intercepted information to the police on the basis that he suspects that the information is relevant to determining whether a criminal offence has been committed.

How does this scenario differ from the current situation?

Currently under the TIA Act, the security firm could access pharmacy employees' communications because they have agreed, under the signed user agreement, to network monitoring.

However, the firm could not undertake any protective action involving copying an incoming email from an external correspondent until that email reaches the mailserver. Any intervention prior to this point would amount to interception under the TIA Act and, potentially, both Peter and the security firm could be prosecuted.

Because the activity leading to the collection of the information is illegal, the information itself would also be affected. Although the information gathered raises the possibility of future criminal activity, currently there is no basis under the TIA Act for Peter to refer the information to a law enforcement agency. Nor could a law enforcement agency give the information in evidence in any prosecution against a person or persons who are using pharmacy client information illegally. This is because the TIA Act states that only lawfully intercepted information can be used for such purposes.

New network protection provisions – Scenario 2

It all started with a harmless bet on Melbourne Cup day. Eric had a lot on at work and wasn't able to make it to the TAB in time, so he looked up who was going to be the favourite and placed a bet over the internet. Next thing he knew, he had won \$100! It was so easy!

Eric didn't have time to look at the horses again until January. It was pretty slow in the office, many people had gone on holiday, and there wasn't much on. Also, Eric had racked up quite a few debts. He decided that he would have another go at the horses, and see how he went.

Over a period of weeks, Eric was hooked. The internet had opened up a wealth of gambling opportunities for him. At first, he tried to limit his gambling to just his lunch hour, but then, well, other people spent ages on the phone, or went for smokos during the day, so why couldn't he just play a quick game of poker?

Trouble was, Eric was looking at sites that were pretty dodgy, and one day he downloaded something onto his computer which made it run quite slowly. He didn't know it at the time, but he had introduced a virus onto his work's computer network which opened a 'back door' onto all the financial files stored on the network. Hackers got in, and stole credit card numbers and personal details of the hundreds of clients which his firm dealt with. Worse still, someone worked out that it was his firm which was the cause of the data loss, and his CEO was furious!

A few weeks later, Eric was stood down. The people in IT Security had traced the virus back to his computer, and had also seen that it was because he had downloaded it from a gambling site. His boss gave him a long talking to. Turns out, IT Security had been watching him for a while – and had even intercepted and blocked some of his attempts to access gambling sites. His boss handed him a wad of paper provided by IT Security which showed just how many times in those past few weeks he had tried to access non-work related sites, and how long he had stayed on them.

Eric left the building in shame. His boss said that the firm was going to take disciplinary action against him – whatever that meant. Eric still had lots of debts to cover and didn't know what to do.

How does this scenario differ from the current situation?

Currently under the TIA Act, although IT Security can set up rules to 'block' Eric's access to certain sites, it cannot intercept him accessing those sites unless a user agreement is in place between Eric and the firm notifying him that all his communications may be recorded. However, IT Security can use the logs of his computer activity to establish the sites Eric has visited and for how long, and provide this material to Eric's boss and any disciplinary process.

IT Security cannot intercept any communication which comes from the sites in response to Eric's actions, for example responding emails and downloaded material, because those sites have no notice that their communications may be intercepted.

Under the new provisions, the firm will be able to intercept all of Eric's communications to websites, and all responding communications from those sites. If Eric has signed a user agreement with the firm that outlines parameters for appropriate and inappropriate use of the network, the firm will be able to use the intercepted material as evidence in disciplinary processes.

Without such a user agreement in place, although the firm could use the intercepted material to assess whether or not Eric was engaging in an inappropriate pattern of behaviour, the material could not be used as evidence in disciplinary processes. The only evidence that could be used in such processes would be information that reached, and was accessed in the firm's computer servers.