CONTRIBUTIONS TO THE JOURNAL

Do you have something to say about law and computers, information technology, the internet or telecommunications? Have you read any interesting cases or books about computers and the law lately? Is there an issue you think would interest your fellow members of the Australian and New Zealand Societies for Computers and the Law?

The Editors encourage all readers to contribute to the Journal. The Editors welcome contributions of any length (from a short case note or book review, to an in-depth article) on any topic relevant to computers and the law.

If you have an article you wish to contribute, or even an idea for an article you would like to discuss, please contact the Computers and Law Journal Editors at editors@nswscl.org.au.

By way of example, following are some topics that could form the basis of an article:

- the Australian Government's review of e-commerce legislation (*Electronic Transactions Act 1999* (Cth) and its state and territory equivalents) and whether Australia should accede to the UN Convention on the Use of Electronic Communications in International Contracts 2005
- the Australian Government's review into the Government's e-security policy, programs and capabilities
- the detection of fraudulent emails
- reforms to the existing telecommunications regulatory regime

Network operators may now intercept to protect their networks

By Anne Petterd

***Anne Petterd** is a Senior Associate in the Sydney office of Baker & McKenzie who practices in the area of information and communications technology.*

Interception laws recently changed to allow network owners and operators to intercept non-voice communications to protect their computer networks. The changes took effect on 12 February 2010. This article outlines and discusses the changes.

The changes amended the *Telecommunications (Interception and Access) Act 1979* (Cth) (***TIA Act***). The federal government considered that the changes were needed to clarify that a person may undertake appropriate activities to protect their network from harmful attack free of the risk of unlawful interception.

Key aspects of the new interception measures are:

- interception is permitted for protecting a network, but it is limited to non-voice communications;
- intercepted information may be used and communicated for network protection purposes; and
- there must be a responsible person for the network who will have identified responsibilities. These include destroying records of intercepted information.

TIA Act network protection challenges

Successive governments have faced the challenge of amending the TIA Act to apply it to new technologies. One of these challenges is striking the balance between the need a network operator has to protect its network from attack (such as by scanning emails for harmful code) and the importance of the sender and recipient of a communication being able to communicate without

unknowingly being monitored, absent extenuating circumstances. As a trial for addressing this issue, the TIA Act was amended in 2006 and again in 2007 and 2008 to in effect allow law enforcement and security Commonwealth and State government bodies to intercept communications passing over their computer networks. However, the changes were temporary and expired on 12 December 2009. The amendments take a different approach to these earlier government-only changes.

The amendments seek to strike the right balance by allowing a limited ability to intercept for protecting a network without needing to consider the sender's knowledge.

Interception regulation

The TIA Act regulates listening to or recording of a communication while it is passing over a telecommunications system without a person's knowledge ("interception").[1] Unless an exception applies, it is illegal to intercept a communication passing over a telecommunications system.[2]

Before the amendments, the interception prohibition presented some challenges for an organisation wishing to monitor its network for harmful code or other attacks on network security. For example, it was uncertain when an organisation could check an electronic communication such as an email for harmful code, once the communication had entered the organisation's network, but prior to the communication being made accessible to the intended recipient. If the email is addressed to an individual, under the TIA Act the communication is taken to be passing over a telecommunications system until it is accessible to the individual.[3] To be "accessible" the communication needs to be:

- received by the telecommunications service provided to the recipient;
- under the control of the recipient; or
- delivered to the telecommunications service provided to the recipient.[4]

Prior to the amendments, if the organisation wished to intercept to check the email for harmful code while the email was in the organisation's system but before the email had reached the mail server (ie, before it was accessible), there was a risk that such a check could be interception and illegal under the TIA Act. It would not be interception if both the sender and receiver knew about the interception. Organisations are able to inform their own personnel whether their communications might be intercepted, however this is not a matter that can always be communicated in advance to the sender of every incoming email.

New network protection provisions

The amendments inserted another exception to the general interception prohibition to allow a communication passing over a computer network to be intercepted and used on a limited basis.[5] As a result of the amendments interception is permitted if it is:

- by a person authorised to perform "network protection duties" for that network. These are defined as duties relating to operating, protecting or maintaining a computer network;[6] and
- reasonably necessary for performing those duties.

The person authorised to intercept may communicate the intercepted information or use it in performing the person's network protection duties.[7] The person may also communicate the intercepted information to:

- the responsible person for the computer network; or
- another person, if reasonably necessary to enable the other person to perform his or her network protection duties for the network.

Those involved in network protection should check if their network protection activities could involve interception (ie, if they are intercepting electronic communications before they finish passing over the communication network). If so, they will need to ensure that the intercepted information is only used and communicated as permitted by the amended TIA Act.

Responsible person for the computer network

The new provisions identify a "responsible person" for the computer network. If the network is operated by or on behalf of a body, its head is the responsible person. Alternatively, the head can designate that a person or people holding particular positions are each the responsible person.[8]

The responsible person for the computer network:

- will authorise in writing who may perform network protection duties for the network;
- must destroy records of intercepted information which are no longer needed.[9] These requirements apply to records held by the responsible person, the network operator or owner and any person performing network protection duties; and
- may communicate lawfully intercepted information to a law enforcement agency. This can occur if the responsible person has reasonable grounds to suspect the information is relevant to determining if a person has committed a "prescribed offence". These are serious offences as detailed in the TIA Act.[10]

The record-keeping and destruction requirements are less onerous than those applying to telecommunications operators. Any organisation wishing to make use of the new network protection provisions will need to put in

place measures that enable the responsible person to comply with his or her obligations.

Voice communications remain off-limits

Under the new provisions, only non-voice communications may be intercepted and used. This means that a person performing network protection duties cannot:

- intercept a voice communication in the form of speech;[11] or
- use or communicate intercepted information obtained by converting a communication into speech.[12]

Government-only appropriate use provisions

The new provisions give Commonwealth and State government bodies with a law enforcement or security role broader rights to intercept and use intercepted information.[13] These bodies are able to give a person additional "network protection duties" to check if an employee, office holder or contractor is appropriately using the body's computer network.

These bodies may instruct a person with network protection duties to intercept to check if the computer network is being appropriately used by a person if:

- reasonable conditions for network use are in place;
- the person using the computer network (ie, the relevant employee, office holder or contractor) has agreed in writing to comply with those conditions; and
- the person complies with those condition in using the network.[14]

If a person lawfully intercepts information in checking appropriate network use, he or she may use or communicate the information for:

- determining whether to take disciplinary action for network use;
- taking disciplinary action if network use is inappropriate; or
- reviewing a decision to take disciplinary action.[15]

In addition to the other restrictions on using intercepted information, the government entities cannot use the information for disciplinary purposes if this would contravene a Commonwealth, State or Territory law.[16] For example, the government body would also need to comply with any applicable State workplace surveillance law.[17]

The extent to which these government-only provisions will be used remains to be seen. The new provisions do not specify the matters that the network use conditions must address or how to assess what are "reasonable" conditions. These uncertainties might make a government employer reluctant to rely on the provisions alone to justify disciplinary action.

Conclusion

The amendments to the TIA Act create a limited ability to intercept for network protection, without imposing a high compliance burden on network operators who choose to do so.

Given the amendments have received little attention, the main issue for network operators may be one of awareness. Those involved in network protection activities need to be made aware of the new provisions so they can check if their current protection measures could be interception and, where necessary, implement procedures to comply with the new laws.

---

[1] See the description of "interception" in TIA Act section 6(1).

[2] Section 7(1).

[3] Section 5F.

[4] Section 5H.

[5] New section 7(2)(aaa).

[6] A definition of "network protection duties" has been inserted in section 5(1). Paragraph (b) contains an expanded definition allowing certain Commonwealth and State government security bodies to also intercept to ensure the network is appropriately used by personnel of those government bodies.

[7] New section 63C.

[8] The definition of "responsible person" has been inserted in section 5(1).

[9] New section 79A.

[10] New section 63C.

[11] New section 7(3).

[12] New section 63C(3).

[13] In an earlier draft of the amendments, these additional powers applied to everyone with network protection duties. However, this proved controversial and was criticised as, for example, giving internet service providers broad rights to intercept to check appropriate network use.

[14] New section 6AAA.

[15] New section 63D.

[16] New subsection 63D(4).

[17] Such as the restrictions on an employer blocking its employees from emails or internet access in section 17 of the *Workplace Surveillance Act 2005* (NSW) and the restriction on use and disclosure of surveillance records in section 18 of that Act.