Australian Government Solicitor the leading lawyers to government

AGS

Commercial notes

Number 13 | **8** February 2005

Online privacy, spam and the Stored Communications Act

Two recent legislative developments herald a new era of parliamentary willingness to address technological issues long claimed by many to be beyond regulation or control. They also mark the end of an age of innocence concerning the consequences of online activities and the beginning of a new era of accountability in Australian cyberspace.

On 14 December 2004, the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* ('the Stored Communications Act') received Royal Assent, resulting in various amendments to the *Telecommunications (Interception) Act 1979* ('the TI Act'). A year and two days earlier, the *Spam Act 2003* received Royal Assent, prior to its commencement on 10 April 2004.

The passing of the Stored Communications Act provides a valuable opportunity to reflect on whether current policies and procedures have kept pace with changes in technology and new legal requirements such as those introduced by the Spam Act in 2004. At the same time, owners and administrators of information technology and communications systems should consider whether there are any additional steps they can take to preserve and protect their IT facilities without breaking the law.

Darwin

Andrew Schatz *Lawyer*
Australian Government Solicitor
T *08 8943 1400* ***F*** *08 8943 1420*
andrew.schatz@ags.gov.au

The Stored Communications Act

The Stored Communications Act will operate for a year from 15 December 2004. During that period, certain stored communications (including certain emails) are excluded from the operative provisions of the TI Act.

The prohibition on interception of communications

Section 7(1) of the TI Act relevantly provides:

> A person shall not:
>
> (a) intercept;
>
> (b) authorize, suffer or permit another person to intercept; or
>
> (c) do any act or thing that will enable him or her or another person to intercept;
>
> a communication passing over a telecommunications system.

Under section 6(1), interception consists of listening to or recording, by any means, a communication in its passage over a telecommunications system without the knowledge of the person making the communication ('the sender'). There are a range of exceptions to the prohibition in section 7(1), but the principal exceptions involve interception under a warrant.

Have your IT policies and procedures kept pace with changes in technology and new legal requirements?

Prior to the amendments introduced by the Stored Communications Act, it was generally unlawful to intercept (without a warrant) any communication passing over a telecommunications system without the knowledge of the sender. This raised some very difficult legal and practical issues in the context of the internet and email with respect to when employers or network administrators could lawfully record communications passing over their networks.

The main difficulty is that, while steps can be taken to notify the people who use an organisation's internet and email facilities that their communications may be recorded prior to delivery, it is practically impossible to warn all potential senders of communications to an organisation that their communications may be recorded prior to receipt.

Not surprisingly, many employers and network administrators were concerned that a number of common administrative practices could breach the TI Act despite the fact they play an essential role in protecting network integrity and limiting the potential for vicarious liability in the event of misuse.

Legitimate reasons for interception

Examples of common administrative practices that may involve recording communications in their passage over a telecommunications system include:

— copying suspect messages that appear to contain viruses, spam or inappropriate material for subsequent inspection by network administrators or security staff

— backing up email servers as a disaster recovery mechanism to guard against data loss

— monitoring internet and email use to ensure users do not damage or misuse telecommunications infrastructure by sending inappropriate, malicious or potentially damaging material

— gathering evidence of misuse or the commission of crimes for later use in criminal or disciplinary proceedings

— running packet sniffing software for diagnostic purposes, to ensure the efficient and effective maintenance of networks or to detect misuse

— in some cases, as an integral function of filtering or blocking technologies designed to protect networks from loss or damage due to spam, viruses and so on.

Employers and network administrators have a legal obligation to supervise and restrict the manner in which their property is used.

Due to the difficulties associated with applying the TI Act to email and internet traffic, some or all of these practices may have been contrary to the TI Act prior to the amendments introduced by the Stored Communications Act.

Despite this, employers and network administrators who provide email and internet access have a legal obligation to supervise and restrict the manner in which their property is used.[1] A number of sexual harassment, anti-discrimination and copyright cases have consistently highlighted the willingness of Australian courts to hold employers accountable for the actions of people who use their email and internet facilities to break the law.[2] Other areas of potential liability include defamation laws[3] and liability for pecuniary penalties under the Spam Act.[4]

Before the amendments introduced by the Stored Communications Act took effect, employers and network administrators seeking to guard their systems against damage or misuse faced difficult choices in their quest to strike the right balance between adequate supervision and protection of personal privacy. Many felt trapped between the laws requiring them to monitor and supervise user activities and the laws restricting the manner in which such monitoring could take place. The Stored Communications Act should make this job easier by providing increased scope for legitimate filtering and monitoring practices, although it should be noted that that is not its primary intent.

The effect of the new provisions

The Attorney-General stated in his second reading speech that the amendments introduced by the Stored Communications Act '*... address obstacles faced by our law enforcement and regulatory agencies ... [and] are an urgent but temporary solution to operational difficulties*'.[5]

The Stored Communications Act amends the TI Act such that 'stored communications' are no longer subject to the general prohibition against interception imposed by section 7 of the TI Act. The term 'stored communications' is now defined in the TI Act as follows:

> 7(3A) ... a *stored communication* is a communication that is stored on equipment or any other thing, but does not include:
>
> (a) a voice over internet protocol (VOIP) communication; or
>
> (b) any other communication;
>
> stored on a highly transitory basis as an integral function of the technology used in its transmission.
>
> Note: Momentary buffering (including momentary storage in a router in order to resolve a path for further transmission) is an example of storage on a highly transitory basis.

Emails on computer hard drives, central email servers or other storage devices are no longer subject to the general prohibition against interception.

Accordingly, since they are not stored on a highly transitory basis, emails on computer hard drives, central email servers or other storage devices are no longer subject to the general prohibition against interception of 'communications passing over a telecommunications system' for the purposes of section 7(1) of the TI Act. Similarly, unread SMS or MMS messages stored on central storage facilities or on mobile phone handsets are also excluded from the general prohibition on interception of communications.

The Stored Communications Act further amends the TI Act such that stored communications are not caught by the term '*lawfully obtained information*' as defined in section 6E. Lawfully obtained information is essentially information obtained by lawfully intercepting communications as opposed to unlawfully intercepting communications in contravention of section 7(1) of the TI Act. The new amendments therefore remove stored communications from the scope of the restrictions on use and disclosure of lawfully obtained information set out in Part VII of the TI Act, clearing the way for them to be used in legal or disciplinary proceedings. However, use and disclosure of stored communications is still subject to the *Privacy Act 1988* ('the Privacy Act') and various other relevant laws.

It is also worth remembering that some monitoring practices may even be unlawful during the period of operation of the new amendments. For example, the use of packet sniffing software for diagnostic or monitoring purposes may breach the TI Act if it involves the real time recording of communications rather than the subsequent copying of stored

communications. Accordingly, employers and network administrators should exercise caution to ensure their activities, however well intentioned, do not break the law.

Finally, the amendments introduced by the Stored Communications Act only have effect for a period of 12 months following their commencement on 15 December 2004. During this 12 month period, the Attorney-General's Department is to conduct a review of the regulation of access to stored communications under the TI Act.[6]

The review may result in more long-term amendments, but if not, the legal position will revert to its previous state on 16 December 2005. Employers and network administrators should bear that in mind when drafting and implementing IT security and acceptable use policies and procedures.

The Privacy Act

In addition to the restrictions imposed by the TI Act, employers and IT administrators considering the extent to which they can monitor the use of their internet and email facilities need to consider the relevant requirements of the Privacy Act.

On 30 March 2000, the Office of the Federal Privacy Commissioner released *Guidelines on Workplace E-mail, Web Browsing and Privacy* ('the Privacy Guidelines'). The publication is available on the Privacy Commissioner's website at <http://www.privacy.gov.au/internet/email/index.html>.

Monitoring and recording practices should only be carried out in a fair and lawful manner.

The Privacy Guidelines provide a useful overview of the manner in which employers and IT administrators can implement logging and monitoring practices without contravening the relevant Privacy Principles set out in the Privacy Act.

The main guideline is that monitoring and recording practices should only be carried out in a fair and lawful manner. Internet and email use should therefore only be recorded after employees and any other relevant users have been put on notice that such recording is likely to take place.[7] IT security and acceptable use policies are helpful in this regard, as are electronic pop-ups and click-wrap agreements requiring users to consent to monitoring and directing them to the location of more detailed policies.

These measures may also have several indirect benefits including a degree of additional protection from the provisions of the TI Act (in certain circumstances) and the ease with which warning messages can be tailored to put users on notice about what constitutes acceptable use. Ensuring users properly understand what they can and cannot do using IT facilities is essential to managing the risk of vicarious liability for inappropriate behaviour while still protecting legitimate rights to privacy.[8]

Once information regarding user activities has been recorded, it should be handled carefully to ensure the relevant Privacy Principles governing storage, use and disclosure of personal information are observed.[9]

Other legal requirements such as those imposed under the *Freedom of Information Act 1982*[10] and the *Archives Act 1983* should also be observed.

The Spam Act

Issue 9 of AGS *Commercial Notes* published on 6 April 2004 and available at <http://www.ags.gov.au/publications/index.htm> contains an overview of the changes government organisations should make to ensure compliance with the Spam Act. Almost a year has passed since the Spam Act commenced, and while many organisations have changed the way they operate, others may not have found the time to make the necessary changes to ensure compliance with their new legal obligations.

As discussed in our previous article, the application of the Spam Act extends beyond the regulation of what is commonly referred to as spam, and it will affect all organisations that use email and internet facilities, including government agencies. It is therefore essential that organisations who have not reviewed their IT security and acceptable use policies since the Spam Act commenced take the necessary steps to do so as soon as possible.

Policy considerations

Leaving legal matters to one side, there are sound policy reasons for government agencies to be seen to be complying with the Spam Act's requirements. In that regard, the Department of Communications, Information Technology and the Arts (DCITA) recently released a publication entitled: *Spam Act 2003 – A practical guide for government* ('the Spam Guide'), available on the DCITA website at: <http://www.dcita.gov.au/ie/spam_home>.

The Spam Guide highlights the importance of government bodies complying with the spirit of the Spam Act rather than relying on the limited exemptions available to them because of their government status. It relevantly states that before relying on the designated commercial electronic messages exemptions set out in clause 3 of Schedule 1 to the Spam Act (which apply to certain messages sent by government bodies), government bodies should be satisfied:

— that the message they propose to send is essential to the work of government, and

— that there is no practical alternate way of complying with the Spam Act's consent requirements.

Organisations should regularly review their IT security and acceptable use policies.

Reviewing IT security and acceptable use policies

Organisations should regularly review their IT security and acceptable use policies to ensure they keep pace with changes in law and technology. The recent reforms brought about by the Spam Act and Stored Communications Act are simply two more reasons to undertake a review aimed at ensuring that all legal risks are covered and that all relevant policies are being adhered to, including those embodied in the Privacy Guidelines and the Spam Guide.

Reviewing IT security and acceptable use policies requires consideration of a range of practical, legal and policy issues. AGS can assist with the process by ensuring that all relevant legal risks are properly identified and addressed at the earliest possible stage. This may be of great benefit to organisations struggling to reconcile unfamiliar laws with rapidly advancing technologies.

Tips for clients

- Review all IT security and acceptable use policies to ensure they do not endorse practices that are unlawful under the provisions of the TI Act.
- Put in place adequate safeguards to ensure employees and other relevant users comply with the relevant requirements of the Spam Act.
- Ensure logging or monitoring practices are carried out in a fair and lawful manner and that they comply with all relevant legal requirements including those imposed by:
  - the TI Act
  - the Privacy Act
  - the Spam Act
  - the Archives Act
  - the Freedom of Information Act
  - all other relevant Commonwealth or State legislation.
- Ensure staff and other users are properly educated regarding what constitutes acceptable and unacceptable use of your organisation's facilities and make sure their knowledge is regularly reinforced through appropriate training sessions and online screen prompts.
- Regularly review policies and procedures to ensure they keep abreast of any new changes in law or technology.
- Watch this space for future updates on the state of the law following the expiry of the amendments introduced by the Stored Communications Act on 15 December 2005.

Andrew Schatz *has an extensive knowledge of technology related legal issues and has worked on a range of IT/IP legal matters. He has degrees in both law and computer science and was recently featured in the 'IT Whiz Kid' section of the ZDNet Australia and Australian Computer Society web sites. Andrew regularly presents on information technology and communications law issues.*

Notes

1 See, for example: 'Misconduct in E-mail and Internet use at Work', AGS *Legal Briefing* No. 58, 27 February 2001; J Catanzariti, 'Being online and staying in line: new technology and the workplace', *Employment Law Bulletin* 6(1) March/April 2000: 1–10; and D Ellinson, 'Employees' personal use of their employer's email system', *Australian Business Law Review* 29(2) April 2001: 165–169.

2 See the reasoning of the High Court of Australia in *University of New South Wales v Moorhouse* (1975) 133 CLR 1, a case involving infringement of copyright using photocopying facilities provided by a university.

3 According to the High Court of Australia in *Dow Jones & Company Inc v Gutnick* (2002) 210 CLR 575, the defamation laws that apply to online material are those of the jurisdiction where the intended recipient receives and views the relevant communication.

4 The various ancillary contravention provisions contained in sections 16(9), 17(5) and 18(6) of the Spam Act arguably provide scope for third parties to be held liable for the actions of people who send contravening messages using their communications facilities.

5 The Hon. Philip Ruddock MP, Attorney-General, *House of Representatives Hansard,* 8 December 2004, pp. 30–31.

6 The Hon. Philip Ruddock MP, Attorney-General, *House of Representatives Hansard,* 8 December 2004, pp. 30–31.

7 See Information Privacy Principle ('IPP') 1 and National Privacy Principles ('NPPs') 1, 10.

8 See, for example: K Levi, 'Guidelines for monitoring workplace emails', *Internet Law Bulletin* 3(4) July 2000; M Paterson, 'Monitoring of employee emails and other electronic communications', *University of Tasmania Law Review* 21(1) 2002: 1–19; and K Eivazi, 'Employees' email privacy and the challenge of advancing technology', *Privacy Law And Policy Reporter* 10(5) September/October 2003: 95–98.

9 See IPPs 4, 9–11 and NPPs 2–4.

10 See *Re Langer and Telstra Corporation Limited* (2002) 68 ALD 762 which dealt with Telstra's obligations to locate and produce emails under section 24A of the *Freedom of Information Act 1982*.

AGS contacts

For legal advice please contact Andrew Schatz of our Darwin office on tel: (08) 8943 1400, email: andrew.schatz@ags.gov.au, or Robert Orr QC of our Canberra office on tel: (02) 6253 7129, email: robert.orr@ags.gov.au or any of the lawyers listed below:

National	Tony Beal	02 6253 7231
Canberra	Jake Blight	02 6253 7035
Sydney	John Berg	02 9581 7624
Melbourne	Kenneth Eagle	03 9242 1290
Brisbane	Robert Claybourn	07 3360 5767
Perth	Lee-Sai Choo	08 9268 1137
Adelaide	Sarah Court	08 8205 4231
Hobart	Peter Bowen	03 6220 5474

For enquiries regarding supply of issues, change of address details etc.

T *02 6253 7052* ***F*** *02 6253 7313* ***E*** *ags@ags.gov.au*

Canberra
50 Blackall Street Barton ACT 2600

Sydney
Level 23, Piccadilly Tower, 133 Castlereagh Street Sydney NSW 2000

Melbourne
Level 21, 200 Queen Street Melbourne VIC 3000

Brisbane
Level 12, Samuel Griffith Place, 340 Adelaide Street Brisbane QLD 4000

Perth
Level 19, Exchange Plaza, 2 The Esplanade Perth WA 6000

Adelaide
Level 20, 25 Grenfell Street Adelaide SA 5000

Hobart
Level 8, 188 Collins Street Hobart TAS 7000

Darwin
Level 3, 9–11 Cavenagh Street Darwin NT 0800

Web site
For a full review of AGS services, visit <www.ags.gov.au>

Electronic versions of AGS newsletters are available for clients who prefer to receive issues in this form. Please contact 02 6253 7052 or email ags@ags.gov.au to arrange supply.

ISSN 1433-9549
Approved Postage PP 255003/05310