Monitoring of Employee Emails and Other Electronic Communications

MOIRA PATERSON*

The use of electronic mail ('email') in the workplace and the provision of access to the Internet are both becoming increasingly prevalent. However, their ease of use, when coupled with the legal dangers which they pose and the illusion of anonymity that such activities create, gives rise to some very complex legal and policy issues. Employers face legal, as well as financial, imperatives to ensure that employees do not make inappropriate use of these facilities and are increasingly resorting to blanket or broad-brush electronic surveillance as a solution. Such an approach may not necessarily be the most effective and exposes them to a number of potential legal pitfalls.

Employers who engage in surveillance activities need to take care to ensure that these do not result in breaches of privacy and electronic surveillance laws. They also need to be aware of the various laws that impose limitations on the uses to which information acquired from the surveillance activities can be put. These laws are by no means straightforward in their operation and are arguably in need of fine-tuning and reform.[1] As noted by the Victorian Law Reform Commission in its Information Paper, *Privacy Law: Options for Reform*:

> Workplace privacy raises difficult questions about the appropriate balance to be struck between employers' claim to exercise management and control over workers, and the rights of employees to have their autonomy and privacy respected and to be treated with dignity.[2]

* Senior Lecturer, Faculty of Law, Monash University and Associate Director of the Centre for Law in the Digital Economy ('CLIDE'). This article is based on a paper presented at the CLIDE seminar, *Current Issues in E-Business*, in April 2001 and has been prepared with research assistance from Ron Ferdinands.

1 The issue of employee privacy is currently under review in Victoria by the Victorian Law Reform Commission ('VLRC'): the terms of reference of its brief can be found at <http://www.lawreform.vic.gov.au/>. See also New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report No 98 (2001) <www.lawlink.nsw.gov.au> at 1 August 2002. Chapter 4 contains detailed recommendations concerning legislative and other measures to ensure accountability by users of surveillance devices, including employers.

2 VLRC, *Privacy Law: Options for Reform* (2001) 48.

In the meantime, it is suggested that the most rational response by employers is to ensure that any electronic surveillance falls within well-documented and carefully articulated management strategies and guidelines. Such strategies should specifically target activities that are contrary to management policy.

The Justifications for Electronic Surveillance

There are a number of common rationales and justifications for employer surveillance of electronic communications. These need to be carefully examined to ensure that responses to them are both effective and not unnecessarily broad.

Performance Monitoring

Surveillance of email and other Internet usage may be carried out as a means of monitoring performance and thereby enhancing productivity. For example, a commonly used software program not only logs all Internet and email use, but also has the ability to record every keystroke, programme used and file opened or copied and to incorporate this information in a searchable report.[3] Products of this type clearly have the potential to improve employee productivity. However, as noted by the New South Wales Law Reform Commission,[4] research indicates that performance monitoring results in psychological and physical health problems that may ultimately lead to increases in absenteeism and employee turnover.[5] In addition, the feeling of continuously being watched can result in a negative workplace atmosphere.[6]

Avoiding Loss of Productivity

A common justification for the use of electronic surveillance is the need to monitor and ensure employee productivity and to make certain that valuable time and resources (including limited bandwidth) are not wasted on personal activities.[7] This is clearly an important issue, but it may be misleading to assess the impact of such activities purely from the standpoint of the amount of time expended on them.

3 New South Wales Law Reform Commission, above n 1, [3.24].

4 Ibid [3.62]-[3.65].

5 J A Flanagan, 'Restricting Electronic Monitoring in the Private Workplace' [1994] *Duke Law Journal* 1256, 1263.

6 Ibid 1264.

7 Ibid 1257.

There can be no doubt that extensive use of email and Internet for purely personal activities will reduce the time available for work-related activities. On the other hand, the opportunity for some personal use may in fact enhance an employee's skills in the effective use of the electronic medium and reduce the amount of time required for personal, face-to-face transactions. For example, an email may replace a longer phone conversation, or the payment of a bill over the Internet may obviate the need to leave the office to pay it at a post office. A more logical approach is to monitor employees' productive output rather than their electronic transactions and to confine surveillance of the latter to situations where there is reason to believe that this may be implicated in a low or reduced level of productivity.

Another related justification is that email surveillance helps employers diagnose internal problems, such as employee morale, as well as measuring individual productivity and assisting them to comply with regulatory requirements.[8] However, while monitoring may serve a useful purpose in helping to achieve legitimate goals such as quality control and minimum service standards, much covert surveillance tends to be based on the dubious assumption that productivity is related to email quality or quantity. It is also open to query as to how effective email surveillance per se is likely to be in achieving employer objectives such as improved morale or increased productivity.

Likewise, if congestion is a major issue, then it may make more sense to tackle it specifically. For example, it may be possible to identify peak periods and to request employees to confine their activities during peak times to those that are strictly necessary. It may also be possible to impose technological constraints, for example, by limiting the size of attachments that can be received. Surveillance could therefore be limited to the context where an employee is detected utilising an unusually large volume of bandwidth during peak times or where their overall Internet usage is unusually large compared with that of their co-workers.

Reducing Legal Risks

A second important justification for electronic surveillance arises from a desire to avoid, or at least reduce, the potential legal liabilities and adverse legal consequences that can arise from employees' use of

[8] See, for example, R G Boehmer, 'Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise From the Modern Sweatshop' (1992) 41 *De Paul Law Review* 739, 745; Flanagan, above n 5, 1257.

email and Internet. The electronic environment presents unique problems in terms of staff management. This is because it makes it possible both for material from within an organisation to be widely disseminated and also for material from anywhere in the world to be accessed and downloaded onto an employer's computer system, both with the mere press of a key or click of a mouse button. Potential dangers include the loss of valuable trade secrets and legal liability for breaches by employees of civil and criminal laws.

The electronic environment poses a threat to trade secrets because the ability of employees to transfer company information that does not have sufficient confidentiality protection to outsiders puts that information at risk of losing its status as a trade secret. Valuable information may fall into the hands of others (including business rivals) either due to misdirection of emails or a failure to take appropriate steps to protect the security of email messages or the security of the computer system on which the information is stored. Not only does this have the potential to 'give away' valuable information, but it also undermines existing protection mechanisms such as pending patents. These issues are dealt with in more detail in the broader discussion of security that follows. However, it should be borne in mind that indiscriminate surveillance will generally be ineffective in preventing specific losses of trade secrets, although it may have a role to play in detecting patterns of suspicious or careless behaviour.

Activities that may create legal liability include the downloading or distribution of copyright materials, the posting of defamatory materials on bulletin boards, the circulation of defamatory material via email, breaches of anti-harassment laws[9] and breaches of obscenity laws (most notably from the downloading of pornographic materials). Again, it is important to ensure that any strategies implemented are both cost effective and specifically targeted at the perceived problem.

The issue of copyright infringement is an important one given the ease with which it is possible for employees to make digital copies not only of text, but also of graphics, software, audios and videos, and also to republish this information to others. While such activities may not attract infringement proceedings when carried out in the employees' own homes (despite their illegality), there is a real risk that copyright owners will seek redress against businesses whose computer systems

9 For example, the Chevron Corporation paid out $2.12 million to settle a sexual harassment case brought by female employees as a result of an email titled 'Why beer is better than women': see A Carson and D Farrant, 'Saving Private E-mail', *The Age* (Melbourne), 4 March 2000, 3.

are detected as engaging in infringing activities. Arguably both education and technology have roles to play in reducing liability. Employees need to be educated not only about copyright but also about the fact that activities which may be tolerated in the private sphere may attract more serious legal consequences when carried out at work. It may also be possible to impose technological restraints on the size and types of files that can be received as email attachments or downloaded from the Internet.

Libel is also an issue of concern given the potential for the widespread publication of injurious information.[10] This may occur accidentally (for example, where a message is inadvertently posted to all members of a distribution list rather than the intended recipient) as well as deliberately. While liability will be confined to jurisdictions where damage occurs, it is possible to envisage circumstances where the person libeled is sufficiently well known to be capable of suffering damage in multiple places.[11] Furthermore, the sorts of lists to which information about another employee is most likely to be sent (for example, internal company distribution lists or distribution lists of persons associated with the company) are those where maximum damage to reputation is likely to occur. Arguably, an employee will suffer serious damage to his or her reputation where the damaging information is distributed to bosses, colleagues and general work associates. However, as with trade secrets, indiscriminate surveillance is unlikely to prevent the publication of the damaging material, especially where the publication is inadvertent.

It may therefore be more effective to devote resources to ongoing education. Employees need to be educated about the potential pitfalls, including the dangers of simply hitting the reply button. They also need to be educated about the fact that materials posted to bulle-

[10] See discussion of the libel proceedings brought by Western Provident Association against Norwich Union at [3.28] of the report by the New South Wales Law Reform Commission, above n 1. See also E Lanyon, 'Jurisdiction and Justice: Challenges in Cyberspace' (Paper presented at the CLIDE Twilight Seminar, Access To Justice: Litigation and ADR Online, Melbourne, 1 October 2001, slides available at <http://www.law.monash.edu.au/clide/papers/slides_lanyon.pdf>); T D Brooks, 'Catching Jellyfish in the Internet: The Public Figure Doctrine and Defamation on Computer Bulletin Boards' (1995) 21 *Rutgers Computer and Technology Law Journal* 461.

[11] See, for example, *Gutnick v Dow Jones & Co Inc* [2001] VSC 305 (28 August 2001), <http://www.austlii.edu.au/au/cases/vic> (leave granted to appeal to the High Court – M99/2001 (14 December 2001), <http://www.austlii.edu.au/au/other/hca/transcripts/2001/M99/3.html> at 4 January 2002).

tin boards and lists can be traced back to their source even where they are posted anonymously.

It is also important for employers to take appropriate steps to prevent the downloading or distribution of offensive matter. Employers need to take reasonable steps to ensure that their computer systems are not used for the purposes of downloading pornography and that employees do not engage in any activities that create a discriminatory work environment. Case law from the United States suggests that email poses particular problems in the context of the circulation of jokes that may be viewed as racially offensive or offensive to women, and via the sending of sexually explicit emails that may be viewed as offensive to women.[12] Once again it is not clear that indiscriminate surveillance will be totally effective in preventing one-off incidents or that it is strictly necessary to avoid problems. What is more essential is to provide ongoing education and also guidelines about appropriate behaviour backed up by effective enforcement mechanisms. The latter may require surveillance where there has been a complaint lodged or where harassment is suspected. It may also be possible to put in place appropriate filtering technologies (for example, ones that detect particular words or graphics). While filters are still something of a blunt tool,[13] they may serve a useful purpose in obviating the need for more indiscriminate surveillance.

In summary, it is doubtful whether indiscriminate across-the-board surveillance is an efficient or effective way of eliminating legal risks. As noted by the New South Wales Law Reform Commission in relation to overt surveillance:

> In its lack of targeting, [it] is analogous to fishing with a fine mesh net. Everything within range is captured, whether relevant to the purpose or not.[14]

For it to serve any useful purpose, it would require considerable resources, including trained personnel and software that is effective in detecting potentially problematic activities. Furthermore, it can be counterproductive in creating a false sense of security not only on the part of the employer but also on the part of employees who may feel that what they are doing is unproblematic if their activities have failed

12 D McGraw, 'Sexual Harassment in Cyberspace: The Problem of Unwelcome Email' (1995) *Rutgers Computer and Technology Law Journal* 491, 497-503.

13 See generally P Greenfield, P Rickwood and H C Tran, *Effectiveness of Internet Filtering Software Products* (2001), a study prepared by the CSIRO for NetAlert and the ABA, accessible at <http://www.netalert.net.au/>.

14 New South Wales Law Reform Commission, above n 1, [3.30].

to attract any adverse reaction. It may therefore be more cost effective to employ educational and technological strategies and to confine surveillance to cases where specific breaches are suspected.

Ongoing education is important in ensuring that employers are aware of how to identify, and deal with, trade secrets, and also of their legal obligations under intellectual property and other relevant laws. It can also play an important deterrent role by making it clear that Internet technology makes it possible for breaches to be detected even after material has been removed or deleted and that infringements may attract potentially heavy penalties. Likewise, as previously noted, technological strategies such as the use of filters may be effective in particular in preventing undesirable activities.

Security

The other main justification for surveillance is the need to protect the security of computer systems. Security threats may arise from breaches of security protocols and from the introduction of computer worms and viruses.[15] Security protocols are important to protect the integrity of computer systems, which may be threatened by the activities of hackers, criminals and disgruntled employees. The risks posed by breaches of security range from the possibility of damage to, or alteration of, important data or systems, theft of trade secrets, fraud and breaches of privacy obligations.

Effective security requires a combination of measures, including the use of firewalls, regular patching of software, use of up-to-date virus scanning programs, use of secure channels of communication[16] and message encryption[17] in respect of communications that contain sen-

[15] One of the most widely known viruses is the Melissa virus, which affected more than 300 organisations, covering more than 100,000 individual hosts: <http://www.cert.org/tech_tips/Melissa_FAQ.html> at 20 December 2002. For details of major viruses in 2001 see S Left, 'Year's top 10 computer viruses named', *Guardian* (London), 28 November 2001, <http://www.guardian.co.uk/internetnews/story/0,7369,608300,00.html> at 12 December 2002.

[16] For example, IPsec (IP Security Protocol) or L2TP (Layer Two (2) Tunneling Protocol). Ipsec is a set of protocols developed to support secure exchange of packets at the IP layer (see <http://www.webopedia.com/TERM/I/IPsec.html> at 20 December 2002) while L2TP is a protocol that enables ISPs to operate Virtual Private Networks (see <http://www.webopedia.com/TERM/L/L2TP.html>).

[17] For example, SSL (Secure Sockets Layer) or PGP. SSL is a protocol developed by Netscape for transmitting private documents via the Internet (see <http://www.webopedia.com/TERM/S/SSL.html> at 19 December 2002) while

sitive information. It also requires that employees should receive ongoing education about the use of secure channels where necessary, the vetting of data in email attachments and data downloaded from the web, and proper care in the selection and protection of passwords.

Indiscriminate across-the-board surveillance may be neither necessary nor fully effective in safeguarding security, and again may be counterproductive by engendering a false sense of security. On the other hand, targeted surveillance will clearly have some role to play where possible breaches have been detected. Some random surveillance may also be required to check for potential vulnerabilities.

Policy Issues

The monitoring of employees' electronic transactions raises complex policy issues because of the vast gap between employee and employer expectations. This arises in part because employees are largely unaware of the imperatives for monitoring and usually abysmally ignorant about the prevalence, ease and scope of monitoring.

One of the reasons for the increased prevalence of electronic surveillance is that the technology makes it not only possible but also comparatively inexpensive to carry out. As a result, there is a growing range of sophisticated new products that are actively marketed to employers, on the basis that they will both improve employee productivity and reduce potential legal and security risks.

Contrary to most employees' expectations, it does not require any level of technological sophistication or a high level of expenditure for an employer to be able to monitor all activities relating to computers, right down to the number of keystrokes.[18] Surveillance may be confined to electronic trails, such as logs of emails (including details of senders, recipients and subject), logs of URLs visited, however fleetingly, and logs of computer usage such as times logged on and off. It can also extend beyond this to details of keystrokes executed, screen content at any given time and email message content.[19] There is now commercially available software that enables companies automatically

PGP is a commonly used, effective, easy to use and free technique developed by Phil Zimmerman for encrypting messages

(see <http://www.webopedia.com/TERM/P/Pretty_Good_Privacy.html> at 20 December 2002).

18 See, for example, the list of products used for monitoring computer use at the Trapware website: <http://www.trapware.com/PressBigBrother.html> at 1 August 2002.

19 Flanagan, above n 5, 1259.

to record, filter and sort every word that streams through their networks. Software can also be used to track an employee's chat room conversations and passwords, and then mail a transcript to an employer. For example, a program currently available at low cost in the United States has been described in the following terms:

> The software covertly detects and documents when an application is opened, who ran it, how long it ran, all window titles, and all keyboard activity. It produces a detailed report on file activity, including all move, copy, delete, and create file actions. Incoming and outgoing e-mail messages are tracked along with web surfing.[20]

Software can also be used to sample content of emails to ensure compliance with an employer's policies[21] and even to monitor instant message exchanges.[22]

Another problem is that many computer users still operate on the false assumption that the requirement to use passwords means that their communications will be inaccessible to their employers. They also tend to assume that evidence of their electronic transactions disappears once they have been completed, or at least where they have taken some positive steps to delete documents or emails. It is not widely understood that information relating to emails is stored outside of the employee's own computer and that 'deleted' messages are in fact still available for months or longer on a backup tape or disk. Likewise, many people are still unaware that it is in fact possible to reconstruct computer files even after they have been 'deleted'.[23]

There are also differences in basic assumptions and expectations concerning rights in respect of computers and computer generated information. It is not uncommon for an employer to take the view that he or she owns the computer system and therefore should have the right to do as it pleases with any information deriving from it. On the

[20] See <http://special.northernlight.com/privacy/index.html>. Further information on the product may be found at <http://www.winwhatwhere.com/>. See also details of the Activity Logger and Activity Monitor at <http://www.softactivity.com/> at 1 August 2002.

[21] See, for example, details about the OTG Software's EmailXaminer product at <www.nwfusion.com/newlwtters/gwm/2002/01228489.html> at 1 August 2002.

[22] M Fordahl, 'Instant message monitoring soaring', *Sydney Morning Herald* (Sydney), 15 April 2002, <http://smh.com.au/articles/2002/0415/1018333471490.html> at 1 August 2002.

[23] For example, see the description of a program called SilentRunner in Ross Haig, 'Computer Forensics Lab Plumbs New Depths of E-mail Evidence,' *The Recorder*, <http://tm0.com/sbct.cgi?s=112051500&i=303816&d=1037246> at 14 February 2001.

other hand, an employee may well assume that information stored within a computer will be treated with the same respect as information stored in a locked drawer (especially where he or she has not knowingly contravened any employer guidelines).

The mismatch between employer and employee expectations creates a situation where employees may be lulled into a false sense of security that makes it possible for them to be monitored and recorded engaging in very personal and private behaviour of the type that they would not ordinarily choose to reveal.

As noted by the Victorian Law Reform Commission:

> personal communications can often involve intimate and sensitive information about individuals and their relationships. They may involve political commentary and criticism. They may also include socially sensitive maters including the fact that an individual is suffering or has suffered from depression, alcohol abuse or illness, or that an individual has a particular sexual orientation.[24]

While it might be expected that people would exercise more caution when using a work computer, email is far closer to speech than a written communication, and typically lacks the care given to a written communication. Its informality, coupled with its ease of use, may result in a greater level of candour about personal matters than would occur in the context of a written letter.[25]

The inadvertent disclosure of personal information is especially problematic as it affects the balance of power and the nature of the relationship between employer and employee. This can occur even where communications are confined to a legitimate business context. For example, an employee who has developed a close rapport with a client may reveal personal information to them in the context of explaining their reasons for preferring to hold a meeting at a particular time or place. There may also be circumstances where it is difficult to draw a clear line between private and business activities or between private time and 'business working hours'. Such blurring typically occurs where a contractor who works from home makes use of the one computer for both personal and work-related activities.

Systematic covert surveillance amounts to a gross infringement of informational privacy – the right of individuals to control how much

[24] VLRC, above n 2, 33.

[25] See, eg, R Dixon, 'With Nowhere to Hide: Workers are Scrambling for Privacy in the Digital Age' (1999) 4 *Journal of Technology Law and Policy* 1, [53]; New South Wales Law Reform Commission, above n 1, [2.43] and references at fn 75.

of their personal lives they wish to share with others.[26] This aspect of privacy has not received much attention until recently as it was protected by the sheer cost and inconvenience of wide-scale monitoring.

Loss of informational privacy is problematic for a number of reasons. First, and most importantly, it makes an individual more vulnerable to discrimination and to exploitation by others such as marketers. Anti-discrimination legislation outlaws the discriminatory use of information relating to issues such as race, disability and sexuality for the purposes of employment-related decisions. However, persons who are discriminated against in employment and other contexts may have no means of knowing, let alone proving, that particular information has been used as a basis for unlawful discrimination.

At a broader level, loss of informational privacy is problematic because of its adverse impact on personal autonomy, integrity and dignity, and consequently on our development as individuals, as well as on our relationships with others.[27] These values may be summed up as being largely concerned with 'achieving individual goals of self-realization'.[28] As noted by the Australian Law Reform Commission, 'claims to privacy are part of the claim that the autonomy of each individual should be protected and his integrity respected'.[29] It therefore follows that privacy claims require, inter alia, that persons should be able to exert an appropriate measure of control on the extent to which their correspondence, communications and activities are available to others in the community.[30]

26 Australia lacks any general common law protection of privacy similar to that which exists, for example, in the United States (although some members of the High Court in the recent case of *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63 left open the possibility of some form of torts protection) and statutes such as the *Privacy Act 1988* (Cth) focus on information privacy/data protections. For a useful discussion of the conception of privacy as information control see: L Bygrave, 'The Place of Privacy in Data Protection Law' (2001) 24 *University of New South Wales Law Journal* 277; S Rodota, 'Protecting Informational Privacy: Trends and Problems' in W F Korthalis Altes, E J Dommering, P Bernt Hugenholtzt and J J C Kabel (eds), *Information Law Towards the 21st Century* (1992) 261.

27 Mark Racanelli describes privacy as a bundle of rights stemming from personal autonomy and personal dignity: M A Racanelli, 'Reversals: Privacy and the Rehnquist Court' (1992) 81 *Georgetown Law Journal* 443, 461-7. See also E Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962; A B Handler, 'Individual Worth' (1989) 17 *Hofstra Law Review* 493.

28 Bygrave, above n 26, citing Alan Westin, *Privacy and Freedom* (1970) 39.

29 Australian Law Reform Commission, *Privacy* (1983) [1032], [1033].

30 Ibid.

The need for control over personal information has been further explained in terms of its relationship to personal identity. Data surveillance creates records containing isolated pieces of information that are used as a basis for making decisions about individuals. Rosen suggests that the growing unease about information surveillance results from justifiable unease about the tendency to view people as the sum of the discrete data held about them:

> As people, we are always far more than the sum of the information that is stored about us. In fact, often too little information is recorded about us to do anything other than create a misleading impression of the kinds of people we are.[31]

Surreptitious monitoring is especially offensive as it reduces both dignity and autonomy. While it is frequently justified on the basis that people should be aware that electronic communications are not a secure medium and act accordingly, this does not accord with reality.[32] Arguably, where an employee is put on notice that surveillance is taking place, the sense of loss of dignity and autonomy may be less harmful since the employee has greater potential to control the degree to which he or she exposes aspects of his or her self to the employer.

An issue that is frequently overlooked is that monitoring also has privacy implications for persons who correspond with employees (including legitimate business contacts) who may reveal information about themselves. It also has implications for the informational privacy of third parties whose affairs are the subject of discussion in any of the communications.

The Legal and Regulatory Framework

The monitoring of employee communications requires not only a consideration of the legality of monitoring (and information gathering) per se, but also of the legality of the conduct that ensues from that monitoring.

31 J Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (2000) 5, cited in T Dixon, 'Valuing Privacy: An Overview and Introduction' (2001) 24 *University of New South Wales Law Journal* 1.

32 A survey by law firm Freehill, Hollingdale & Page (as it then was) released in February 2000, which was noted by the New South Wales Law Reform Commission, above n 1, [2.44], found 76 per cent of organisations polled periodically monitored email. However, only 35 per cent informed customers or staff about it. See also K Levi, 'Guidelines for Monitoring Workplace Emails' (2000) 3 *Internet Law Bulletin* 59.

Monitoring/Data Gathering

There are two specific laws that impose legal limitations on the monitoring of communications and data gathering more generally: the *Telecommunications (Interception) Act 1997* (Cth) and the *Privacy Act 1988* (Cth) as amended by the *Privacy Amendment (Private Sector) Act 2000* (Cth).

The *Telecommunications (Interception) Act 1997* s 7(1) prohibits the interception of communications *passing over* a 'telecommunications system'.[33] The 'interception of a communication passing over a telecommunications system' consists of listening to or recording, by any means, such a communication in its passage over that telecommunications system without the knowledge of the person making the communication (s 6(1)).

The prohibition against interception would appear to encompass all equipment within Australia up to and including a user's computer, connected to the Internet. It is less clear, however, how much of the message information it protects. For example, it is unclear whether it extends to the IP headers of emails, although it clearly encompasses the body/content of the emails themselves. It also arguably applies to all of the Australian Internet, all computer networks within Australia and all computers within Australia that are linked to the Internet. However, it is only illegal to intercept a message that is passing over the system at the time of the interception – there is no prohibition on accessing communications once they have in fact arrived.[34]

The other legislation that impacts on the gathering of information is the newly amended *Privacy Act 1988* (Cth). Recent amendments impose for the first time on the private sector (other than the personal credit reporting industry, which has been subject to regulation under the Act since 1993) a set of privacy principles which include restrictions on the gathering of data. However, the new provisions do not apply to acts or practices 'directly related to an employee record' provided that they are 'directly related to a current or former employ-

[33] The latter term is defined as a 'telecommunications network' – that is, a system or series of systems for carrying of communications by means of guided or unguided electromagnetic energy or both, that is within or partly within Australia: *Telecommunications (Interception) Act 1979* (Cth) s 5(1).

[34] For more detailed discussion of the control of communications interception pursuant to telecommunications legislation see R Magnusson, 'Privacy and Surveillance in Australia's Changing Telecommunications Environment' (1999) 27 *Federal Law Review* 33; N Waters, 'Telecommunications Interception – Extending the Reach or Maintaining the Status Quo' (1997) 4 *Privacy Law and Policy Reporter* 110.

ment relationship between the employer and the individual'.[35] In other words, former and current employees lack any informational privacy rights where the information in question relates to their employee record. The requirement that there must be a direct relationship to an employment relationship is somewhat vague, but it would, for example, encompass monitoring associated with matters such as an employee's performance or conduct.

While the employment record exemption does not cover contractors, sub-contractors or prospective employees, the private sector amendments do not extend to businesses that have an annual turnover of less than three million dollars.[36] So-called 'small' businesses are not subject to the National Privacy Principles in the *Privacy Act 1988*, although they are subject to restriction preventing the commercial use of personal records (for example, by selling them to direct marketers).

Uses of Data Gathered

The data gathered as a result of monitoring activities may be used for a variety of purposes and it is especially important to ensure that these do not fall foul of the law. Those likely to create the greatest difficulties concern the use of data to penalise or sack employees or to discriminate against them in some way, and the dissemination of data to third parties. There may also be potential liabilities vis-à-vis third parties whose activities are monitored in the course of monitoring employees' communications, although it is unlikely that they would be able to establish damage or other harm in the absence of dissemination or other unusual circumstances.

The potential dangers of using data as a basis for taking action against employees for breach of guidelines relating to electronic communications is highlighted by the decision of the Federal Court in *Australian Municipal, Administrative, Clerical & Services Union v Ansett Australia Ltd.*[37] This case turned predominantly on issues relating to the sacking of an employee for trade union activities, but the court emphasised the importance of bringing any such guidelines to the attention of employees. Employers who monitor employee activities with a view to taking disciplinary action against those who fail to abide by company guidelines generally need to ensure that they can prove that the employee in question was fully aware of the requirements. They

35 *Privacy Act 1988* (Cth) s 6.

36 *Privacy Act 1988* (Cth) s 6D.

37 [2000] FCA 441.

also need to establish that he or she has previously received some formal warning. In other words, in addition to having Internet usage guidelines, they need to ensure that they also have in place and apply adequate procedural fairness policies.[38]

There have been a number of reports concerning the sacking of employees for downloading or distribution of pornography. While it is usually easier to make out a stronger case for dismissal where activities are illegal on the ground that there is no reasonable basis for any assumption that such behaviour is permissible, employers should make it very clear exactly what is and what is not acceptable. (It is also a good idea to install filtering software that warns an employee that they may be entering a forbidden site or that their email contains unacceptable language.) Guidelines can be problematic to the extent that they are confusing and even contradictory: for example, they may state that specific behaviour is forbidden and then imply that it may be permissible in certain circumstances.

The dissemination of data to third parties also raises some complex issues. The *Privacy Act 1988*, including National Privacy Principle 2[39] which restricts uses and disclosures of information, will apply to activities that are not directly related to employee records, at least in the case of employers who do not fall within the small business exception.[40] To qualify for the small business operator exemption, a business must have an annual turnover of three million dollars or less and must not be related to a business with an annual turnover of greater than three million dollars. In addition, it must not provide a health service; hold health records; disclose personal information about an individual for a benefit, service or advantage; provide a benefit, service or advantage to collect personal information; or be a contracted service provider for a Commonwealth contract. In summary, this means that a business cannot sell or otherwise deal in a commercial manner with employee data gleaned via monitoring activities as this will, in the absence of clear consent, fall foul of privacy principles embodied in the Act.

[38] J Nolan, 'Privacy in the Workplace, Part 3: Some Legal Issues' (1995) 2 *Privacy Law and Policy Reporter* 48; Levi, above n 32.

[39] The National Privacy Principles are contained in Schedule 1 of the *Privacy Act 1988* (Cth).

[40] Section 13A(1) provides that the Act applies to acts and practices of an 'organisation', which is defined in s 6C(1) to exclude a 'small business operator' as defined in s 6D. The employee record exemption is contained in s 7B(3).

The dissemination of data gathered from monitoring activities (whether relating to employees or third parties) may also give rise to potential liabilities vis-à-vis those information subjects. For example, if the information was surreptitiously gathered concerning a confidential communication to a third party, then its dissemination may give rise to an action for breach of confidence in circumstances where the employee can establish some detriment. There is also obvious potential for defamation proceedings. Employers should also bear in mind that, while the provisions in the amended *Privacy Act 1988* which allow for access to personal records are subject to a number of exceptions,[41] they will make it easier for individuals to gains access to their personal files, including data supplied by third parties.

Measures That Can be Taken to Reduce Potential Legal Problems

Employers who choose to survey their employees' electronic communications can reduce potential legal problems by ensuring that their practices comply with the *Guidelines on Workplace E-mail, Web Browsing and Privacy*, which were issued by the federal Privacy Commissioner in March 2000.[42]

This document contains the following 6 basic guidelines:

1. The policy should be promulgated to staff, and management should ensure that it is known and understood by staff.
2. The policy should be explicit as to what activities are permitted and forbidden.
3. The policy should clearly set out what information is logged and who in the organisation has rights to access the logs and content of staff email and browsing activities.
4. The policy should refer to the organisation's computer security policy.
5. The policy should outline, in plain English, how the organisation intends to monitor or audit staff compliance with its rules relating to acceptable usage of email and web browsing.
6. The policy should be reviewed on a regular basis in order to keep up with the accelerating development of the Internet and information technology.

41 See National Privacy Principle 6.

42 These can be accessed at <http://www.privacy.gov.au/internet/web/index.html>.

Translated into practice, this suggests that employers who have not already done so should consult with employees to develop an acceptable use policy that defines precisely what is and is not allowed.[43] (For example, if the policy proscribes non work-related activities, the terms 'work-related' should be clearly defined.) Employees should be informed that any use of their email or Internet facilities will be taken to have been made by them. They should also be provided with details of the range of persons who are authorised to monitor and review their activities and of the types of uses to which surveillance information may be put. Such a policy should be separate from the company's privacy policy and should ideally appear on screen whenever users log on to use the computer. It should also be updated as required to reflect relevant technological developments.

While the Privacy Commissioner's guidelines are not enforceable against private sector bodies, they serve as a 'guide to good practice'[44] and compliance with them would considerably reduce the scope for problems of the type encountered in *Australian Municipal, Administrative, Clerical & Services Union v Ansett Australia Ltd.*[45]

Employers may also find it useful to refer to the more expansive draft code of practice, *The Use of Personal Data in Employer/Employee Relationships*, which has been issued by the United Kingdom Information Commissioner.[46] This suggests the following useful factors to bear in mind when implementing or revising monitoring and acceptable use policies:

- The risks that might be controlled should be carefully and realistically evaluated when assessing the benefits of monitoring communications.
- Care should be taken to ensure that employees are not misled (whether by action or inaction) into false expectations that their communications are private.
- Policies on Internet access should as far as possible be enforced by technical means to restrict access rather than by monitoring behaviour.

[43] For a useful discussion of the arguments favouring employee participation in defining e-policies see J P Kesan, 'Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace', University of Illinois Law and Economics Research Paper No. 00-32, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=289780> at 4 August 2002.

[44] New South Wales Law Reform Commission, above n 1, [4.74].

[45] [2000] FCA 441.

[46] This can be accessed at <http://www.dataprotection.gov.uk/dpr/dpdoc.nsf>.

- In using the results of any monitoring it is important to take account of the ease with which websites can be visited unwittingly through unintended responses of search engines, unclear hypertext links, misleading banner advertising or miskeying.
- In deciding whether or not to prohibit personal use it needs to be remembered that email and the Internet are now routinely used for a number of transactions that were previously conducted by mail or face-to-face and that many employees work for very extended hours.

A third valuable source of principles can be found in the International Labour Office's code of practice on the protection of workers' personal data.[47] This is a voluntary code intended, inter alia, to provide guidance in the development of work rules, policies and practical measures in the workplace.

The principles contained in the code include requirements that personal data should be processed lawfully and fairly[48] and that data collected in connection with measures to ensure the security and proper operation of automated information systems should not be used to control workers' behaviour.[49] The code also requires, inter alia, that:

- Employers should regularly assess their data processing practices so to reduce as far as possible the kind and amount of personal data collected and to improve ways of protecting workers' privacy.[50]
- Workers and their unions should be kept informed of any data collection process and the rules that govern it and about their rights in relation to those processes.[51]
- Workers, without first having to ask, should be regularly notified of personal data held about them and the processing of that data.[52]

47 International Labour Office, *Protection of Workers' Personal Data* (1997). For a general overview see P Roth, 'The International Labour Office Code of Practice on the Protection of Workers' Personal Data' [1998] *Privacy Law and Policy Reporter* 34.

48 Clause 5.5. See also clause 6 concerning the collection of information.

49 Clause 5.4.

50 Clause 5.7.

51 Clause 5.8. See also clause 6.14(2), which requires employers to minimise the intrusion to the privacy of workers resulting from any monitoring and to inform them and their representatives of the reasons for monitoring, the time schedule, the methods and techniques used and the data to be collected, and clause 6.14(3) which permits continuous monitoring only if required for health and safety or protection of property.

Conclusion

The legal and regulatory framework regulating monitoring by employers of emails and other electronic communications is still very fragmented and incomplete.

While there are, in general, few legal limitations on the ability of private sector employees to monitor electronic communications, there are many important limitations on the uses to which information gleaned from monitoring can be put.

The ultimate goal should be to strike an appropriate balance between employer interests and employee interests in privacy, 'a balance that, in the end, allows for surveillance under certain limited conditions, stressing less intrusive approaches'.[53]

It is suggested that carefully drafted guidelines can play a useful and valuable role in achieving this objective. The drafting and dissemination of guidelines serve invaluable educative roles for employers and employees respectively, while providing a better understanding of their mutual obligations. They also provide a useful reference point for determining the appropriateness of employee conduct in the event of any disputes.

[52] Clause 11.8.

[53] D A Cozzetto and T B Pedeliski, 'Privacy and the Workplace: Technology and Public Employment', <http://www.ipma-hr.org/pubs/cozzfull.html> at 20 December 2002.