

Email and the internet: Are expectations of employee privacy realistic?

The widespread use of email and the internet at work is putting the conventions and expectations of employee privacy to the test. Email, particularly, offers employers a technical capacity for surveillance that has not previously existed. Most employees have an expectation that they will be able to maintain some privacy at work. This expectation is often reinforced to employees through the allocation of private drawers and lockers in some workplaces, in other cases through password access to computer systems. Most employers also tolerate and approve some limited use of the telephone for necessary private calls. In the 1995 Australian Workplace Industrial Relations Survey (AWIRS) 74 percent of employees believed they would be able to use a phone at work for family reasons. Although these expectations are widespread, they are not, in fact, grounded in any legal right to privacy for personal mail received at work. Email and internet usage has made the ambiguities surrounding these issues surface, on occasions leading to burnt fingers for both employers and employees.

The use of email and the internet in the workplace has now become a common place occurrence. In fact, the use of these facilities is considered, in many circumstances to give firms a competitive edge. Last year, large employers such as ANZ, BHP and Ford all announced large scale incentive schemes to encourage their workers to become fluent in internet and electronic forms of communicationsⁱ. While the use of these technologies is expanding, and often actively encouraged by employers, the legislative framework to interpret and deal with the privacy implications of these technologies has not yet been developed.

Is email as private as a phone call?

The technology associated with email, and the use of internet facilities means that communication can be monitored in an unprecedented way. The Privacy Commission guidelines broadly distinguishes the new technology, from other types of communication devices, in three main waysⁱⁱ.

- ? Email is insecure because it can be read during transmission (if stored on a server) and can be read by anyone who receives it. An email can be read without the intended recipient having any knowledge of the message being intercepted. Reading an email in this way is easier than steaming open a letter!

- ? Emails cannot be destroyed. Deleted electronic documents can be traced and recovered by information technology staff.

? A detailed history of all email communication, including web activity, is usually logged. These logs usually include lists of sender and recipient addresses and times and dates of transmission.

Ambiguity over monitoring of email and internet use

Legal experts and practitioners have been vocal in exposing the inconsistency in the treatment of email, compared to other forms of communication used in the workplace, such as the telephone. As Professor Ron McCallum points out, the Commonwealth Telecommunications (Interception) Act 1979 “...*does give users of the telephone some privacy by forbidding telephone interceptions of external telephone calls*”ⁱⁱⁱ. There is currently no legislation making it illegal for an employer to monitor employee emails, if the employer owns and operates the email server.

However, other practitioners argue that the assumption by employers that the monitoring of emails can occur with impunity, is flawed. At the Queensland IR Society Convention held in November last year, Minter Ellison lawyer Megan Dixon proposed that the Telecommunications (Interception) Act 1979 could apply to email traffic^{iv}. Under the definitions of a ‘telecommunications system’ applied by the Act, the employer’s network server might be considered to comply with this definition. If this is proved to be the case, storing copies of emails, intercepting and monitoring email communications could be considered illegal under the Act. A major point of contention appears to hinge on achieving or receiving the consent of the originator, before monitoring occurs.

Lessons for employers

There is a danger for employers in *not* monitoring email and internet traffic. In the case of sexual harrassment and discrimination, employers may be held liable if they have not taken reasonable steps to prevent or intervene in the distribution of offensive material. As lawyer Megan Dixon states however, there is no established case law that could be used to define ‘reasonable steps’ necessary, under these circumstances, to prevent sexual harrassment.

Cases heard by the Federal Court last year show that employers must carefully consider the use of information acquired by monitoring email communications^v. In a highly publicised case, Ansett objected to the content of a union bulletin distributed over the internet, and consequently sacked the union delegate for using the email service to distribute union material. The Court found the dismissal to be unlawful because the employee’s use of the email to distribute union material had been reasonable for two main reasons. Firstly, a joint working group had been established at the work site, so Ansett had ‘impliedly permitted’ the use of email communications. Secondly, the union should be entitled to provide feedback and distribute material on meeting outcomes, in the same manner as the employer. Justice Ron Merkel was keen to point out that the

decision should not be interpreted as an authorisation for unions to use the employer's email service to distribute email material. The Justice stated "*Whether an authorisation exists will depend upon the particular circumstances of the case*"^{vi}.

Lessons for employees

For employees, there appear to be two important lessons to take heed of. The first is to understand workplace policies regarding email use – should these exist. The second lesson is to not assume that privacy will be maintained. In December of last year, the IRC upheld a decision by Toyota to dismiss two employees for distributing pornographic images across the company's email system. Toyota dismissed the employees in September for the sending of pornographic images via email, and the storage of offensive images on PC hard drives and floppy disks. The decision to dismiss was upheld for a number of reasons. Senior Deputy President Ian Watson, stated that the sending of such images alone was a reasonable ground for dismissal. More importantly however, Watson stated that the employees should have been aware of the equal opportunity policies in place at the workplace, and must have seen electronic 'pop-up' messages that reminded employees of the Toyota's policy with regard to internet and email usage. The policy warned employees that internet mail messages were not private, that Toyota had the facility to retrieve deleted mail, and that transmissions may be monitored. With regard to offensive material, the policy also explicitly stated that "*Under no circumstances shall Toyota's electronic communications systems (Internet, Intranet, email, telephone) be used inappropriately, including for the following purposes:...to access and/or download pornographic material*"^{vii}.

Privacy Commission guidelines

These issues are unlikely to be resolved entirely by legislation, despite the introduction of new privacy legislation in 2000. The Privacy Amendment (Private Sector) Act 2000 will regulate the collection of *personal* information, and how this information can be used and stored by organisations. However, the legislation has a strong focus on medical records, rather than wider issues relating to employees. There are also many small employers who will be exempt from the legislation.

There appears to be some consensus emerging among legal practitioners and experts on workplace practice regarding email and internet usage in the workplace. *Each workplace should develop guidelines for the use of electronic mail service and the internet, and that staff be properly informed of these guidelines.* In the Ansett case (discussed earlier), the Federal Court strongly advised employers to develop policies on email systems. The Privacy Commission also gives strong support to this view, and has developed a series

of guidelines to assist employers to develop and improve existing policies. The guidelines broadly argue that:

- ? Management should ensure that a policy is known and understood by all staff. The policy should, ideally, be linked to a screen the user will see when logging into a network.
- ? The policy should state permitted and forbidden activities.
- ? The policy should state what information is logged and who has the right to access the logs and content of staff email and internet activities.
- ? The organisation's computer security policy should be outlined in the policy.
- ? Any intentions to monitor or audit staff compliance with the policy should be stated.
- ? Provisions to periodically review the policy should be put in place.

Obviously these guidelines do not resolve the difficult issue of whether employees should be entitled to privacy, and how far this entitlement should extend. However, these guidelines may help to resolve some of the immediate ambiguities that currently exist, and have the potential to prevent significant disputes between the employer and employee.

ⁱ See 'ANZ subsidises employee internet access and PCs' Workplace Express, 31 March 2000. www.workplaceexpress.com.au

ⁱⁱ See The Australian Privacy Commissioner's website. <http://www.privacy.gov.au>

ⁱⁱⁱ Professor Ron McCallum. Presentation to the Employment Law IIR 2001 Conference Sydney, Mercure Hotel 23 February. Title: 'Regulating personal use of email and the internet: where to draw the line?'

^{iv} See 'Email/internet screening: is it legal?' Workplace Express, 6 November 2000. www.workplaceexpress.com.au

^v See *Australian Municipal, Administrative, Clerical and Services Union v Ansett Australia Ltd* (2000) 175 Australian Law Reports, 173.

^{vi} As cited in 'Tell employees rules on email, court urges' Workplace Express 9 April 2000. www.workplaceexpress.com.au

^{vii} See 'IRC upholds email porn dismissals' Workplace Express 20 December 2000. www.workplaceexpress.com.au