Big Brother

By
Dr Rosanna Cooper
First Published by Chemistry in Britain, 2001

Do you know if your e-mails are read by your employer? Rosanna Cooper explains how recent legislation protects both you and your employer

Has your company implemented an e-mail or internet policy and if so, are you aware of the implications of breaching such policies? Recently there has been a spate of well-publicised cases where employees abused their employers' e-mail policies, resulting in the eventual termination of their employment.

The abuse of e-mails and the illegal use of the internet are serious issues that employers have to address. To what extent can an employer go to stop employees? Does the law allow employers to intercept and monitor employees' e-mails and their use of the internet? Four pieces of legislation have recently been implemented in the UK, and have had a tremendous impact on this area:

- the Regulation of Investigatory Powers Act 2000;
- the Data Protection Act 1998;
- the Human Rights Acts 1998; and
- the Telecommunications (Lawful Business Practice)/(Interception of Communications) Regulations (TLBP).

Under the Regulation of Investigatory Powers Act 2000 (RIPA), it is an offence for employers unlawfully to intercept public telecommunication systems unless they have reasonable grounds for believing that there was consent to the interception. Because most businesses found it difficult to prove that they have had an employee's consent, new legislation was introduced in the form of the TLBP. The TLBP allows businesses to intercept and monitor employees' communications, including external e-mails and the use of internet for commercial purposes. However, any monitoring or interception has to be compliant with regulatory practices and procedures.

The primary role of the TLBP is to safeguard the confidentiality of employees' communications and their right to personal privacy. Employers are only able to intercept an employee's e-mails where they can prove that the evidence collected from the interception outweighs the confidentiality or privacy of that employee.

The Data Protection Act 1998 (DPA), protects individuals against companies divulging or using any of their sensitive and personal data. Following the recent implementation of the DPA, a consultative draft Code of Practice (Code) was

introduced specifically to deal with the issues of monitoring employees' e-mails. The Code aims to permit employers the right to monitor their employees' e-mails but only if there is no other way to address the problem. For example, if an employer considers that an employee is spending excessive time disseminating information in external e-mails, they could monitor that employee's e-mail traffic rather than read each individual e-mail. This would avoid any breach of the employee's right to privacy.

Article 8 of the Human Rights Act 1998 (HRA), protects an employee's right to privacy and family life. The HRA may be relevant to any employer whose role includes public functions such as privatised industries and other organisations under contract to central or local government. The only exception to this is where the interference is in the interest of the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of individuals. Courts and tribunals have to interpret the law in the light of the Human Rights Convention, and employers must therefore be fully aware of the provisions of the HRA. In one case the Merseyside Police intercepted office telephone conversations by one of its employees by the name of Halford, who then made a complaint against them. The court held that the interception was a violation of Article 8 of the HRA and Halford was awarded £10,000. Following this, the Home Office issued guidelines on the interception of telephone calls.

Employees should expect to have some degree of privacy in the workplace, unless they are made aware that monitoring could take place. Employers should give adequate warning that interception might take place and should obtain written consent where appropriate. The warning should be set out in e-mail policies and/or contracts of employment.

Generally, e-mail policies are standard to any industry sector, including the chemical industry, and should include the following:

- the intention of the company in producing such a policy;
- whether personal use is permitted and some guidelines as to what is permitted by employees;
- whether confidential information may be sent by e-mail or not;
- employees' responsibilities regarding security of their terminals and passwords;
- whether the company will be monitoring e-mails and what right the company has to monitor their employees' use of e-mails;
- the types of misuse that would result in gross misconduct or disciplinary action; and
- a statement that e-mails should be of the same standard as any other form of communication.

Employers should adopt e-mail policies or existing policies should be reviewed in the light of the recent legislation. These policies should state clearly what

employees are allowed to do in relation to the use of e-mails and whether monitoring will be carried out. However, employers must ensure that the protection of their commercial interest is proportionate to the monitoring and interception in the light of what they are required to achieve in compliance with existing legislation. Employees must be aware of their employers' e-mail policies and abide by them, otherwise they risk losing their jobs.

Rosanna Cooper is a partner at RT Coopers Solicitors, solicitors specialising in intellectual property and technology; tel: + 44 (0) 207 488 2985; e-mail: r.cooper@rtcoopers.com