

# E-MAIL MONITORING - II

## A HARASSING CASE OF CONFUSING MESSAGES

Jonathan Tait

Continuing the theme explored in the previous paper, this article considers how companies should be encouraged to respond to the threats posed by eavesdropping at work.

E-mail misuse and sexual or racial harassment via E-mail are increasingly resulting in legal liability lawsuits. Multi-million dollar penalties appear to have grown in line with the growth of Internet usage itself, and the resultant damage to company reputation is immeasurable.

As examples:

- **Nissan Motor Company.** Two Nissan employees were fired for sending sexually explicit E-mail messages but subsequently sued for unfair dismissal, claiming violation of privacy. (Nissan won the lawsuit because it had an E-mail policy in place that prohibited the use of company-owned computer systems for non-company business.<sup>1</sup>)
- **BG.** Distribution firm BG paid out a \$161 000 libel settlement to rival Transco, after a BG senior manager sent an E-mail, deemed to be defamatory, to Transco staff wrongly suggesting that Exoteric Gas Solutions (created by BG) had misused confidential information from Transco.<sup>2</sup>
- **Chevron.** In 1995, the Chevron Corporation, USA paid \$2.2 million to four female employees after the women claimed they were sexually harassed with E-mail jokes.<sup>3</sup>
- **Norwich Union.** Norwich Union Insurance made a £450 000 out of court settlement for alleged defamation by E-mail against Western Provident Association.

### UK HUMAN RIGHTS ACT/RIP LEGISLATION

Whilst these are important precedents, on 2 October 2000, the Human Rights Act 1998 came into force in the UK. Protected by the European Convention on Human Rights (ECHR), the legislation could affect employers' rights to intercept an employee's personal E-mail at work. The Regulation of Investigatory Powers (RIP) Bill came into effect later the same month providing businesses with legal recourse against the misuse of power by bodies exercising regulatory powers which unlawfully intercept E-mail communication.

Article 8 of the Human Rights Act ("Right to respect for private and family life") states the following:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the eco-

nomical well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The term 'correspondence' could refer to personal telephone calls and E-mail at work. This is the only article that could legally be interpreted in respect to the Human Rights Act to include the interception of an employee's personal E-mail at work.

In statement 2, the term 'public authority' covers not just Government departments, but also privatized public companies (such as utilities companies and Railtrack), NHS Trusts and regulatory bodies, for example.

This is where the RIP Bill interfaces with the Human Rights Act. The Government intends the law to help tackle illegal online activity and to track down criminal behaviour. Whilst it will make it easier for the State to monitor and prosecute criminals, the additional police power has caused much controversy. Many see little relief in the fact that a surveillance warrant will need to be issued and the sender or recipient of an E-mail will be able to claim for damages if they can prove that they have suffered a loss as a result of unlawful interception.

### COMPANIES' RESPONSE TO THE ACT

Organizations have a duty to inform employees on appropriate and inappropriate use of company E-mail systems, including both business and personal E-mail. To meet the requirements of the Human Rights Act (HR Act), while protecting both the organization and its employees from content security threats, it is recommended that a company instigate an E-mail and Internet usage policy.

Provided that a company's written E-mail policy has incorporated the requirements of the HR Act and communicated this to employees (for example, to stop managers intrusively monitoring staff personal mails), the use of E-mail monitoring software to enforce it remains legal. And indeed it may help prove consistency in dealing with employees who abuse the system and demonstrate responsible practice.

In the UK, employers have always been responsible and liable for the actions of their employees. However, if organizations can demonstrate a 'duty of care' to reduce unacceptable employee activity online, then they could minimize its potential for liability.

## E-MAIL AND INTERNET POLICIES

Manufacturers such as Content Technologies have underlined the importance of such policies. Content Technologies' recommends a simple three point process: establish, educate and enforce.

*Establish:* A good policy will protect both the organization and its employees from various content security threats, including loss of intellectual property, offensive and inappropriate materials, legal liability and viruses. With respect to the HR Act, it is vital that companies clarify, with the use of examples, exactly what is deemed by the company to be acceptable and unacceptable use of the business E-mail system with regards to personal usage. Policies need to be defined and implemented with the support of IT, Human Resources and Senior Management and should cover both the management and staff perspectives.

*Educate:* A clear and precise E-mail policy, which also offers the rationale behind the policy, will help gain employee support and approval. It may allay any fears employees have about E-mail content scanning, and set expectations with regard to privacy and the benefits extended to the employee by the policy as well as to the organization as a whole, such as protection from racial and sexual harassment. The policy should also be easily accessible to all employees to read (e.g. on the network) at any time.

*Enforce:* The best way to enforce an E-mail usage policy, and probably the only way to ensure consistency, is to implement a centrally managed policy-based E-mail security solution. It can be customized to fit the company's written E-mail policy and can be modified to allow for company policy changes or amends to legislation.

## MANAGING AN E-MAIL POLICY

To manage an E-mail policy successfully, the following may help:

- Schedule regular reviews.
- Ensure board level support for the policy and any changes to it. These changes must be properly communicated.
- Remind employees of the policy. A simple policy booklet to highlight acceptable and unacceptable E-mail, Web and encryption usage could be given to new employees. E-mails can be used to remind employees of the policy. And posters displayed around premises can highlight particular aspects.
- The policy should become part of a legally binding agreement between an employee and the company through, for example, an employee acknowledgement agreement.
- Schedule regular training, allowing time for questions and feedback.
- Make all statements clear, timely and achievable.

**Jonathan Tait** is European Product Marketing Manager for Content Technologies, a Baltimore Technologies company and developer of E-mail and Internet security and policy management solutions.

Further examination of the issues, white papers, legal text and resources to help fight E-mail and Internet misuse can be found on the Content Technologies website: <[www.mimesweeper.com](http://www.mimesweeper.com)>.

### FOOTNOTES

<sup>1</sup> January 2000, Human Rights (USA) / Computer Weekly.

<sup>2</sup> January 1999, Human Rights (USA).

<sup>3</sup> November 1998, The San-Diego Union-Tribune, USA.

## Book Review

### Multimedia

**Perspectives on Content-based Multimedia Systems**, by Wu, Kankanhalli, Lim and Hong, 2000, hard-cover, Kluwer Law International, 391 pp., £81, NLG290, US\$115, ISBN 0 7923 7944 6

This book is about the resolution of practical problems associated with the building of content-based multimedia systems. Formalizations of the process to bring it to a sufficient level of consistency and integrity are essential to the success of the project. The content-based access to multimedia data is of primary importance and it is the natural way by which human beings interact with such information. With decreasing costs of consumer electronic devices, such as digital cameras and digital camcorders, together with the ease of transportation facilitated by the Internet, there has been a phenomenal rise in the amount of multimedia data generated and distributed. A clear means is therefore needed for capturing, storing, indexing, retrieving, analyzing and summarizing such data. This book covers the research results, making them accessible to practitioners in computers science and electrical engineering.

Available from Kluwer Academic Publisher Group, Distribution Centre, PO Box 322, 3300 AH Dordrecht, The Netherlands; Tel: +31 78 6392 392; Fax: +31 78 6392 254; E-mail: [services@wkap.nl](mailto:services@wkap.nl).