Under surveillance

How can organisations monitor employees' Internet and email activities for abuse, without infringing their right to privacy?

Mention email monitoring to many employees, and talk of Big Brother and police states often follows. When the UK Parliament passed the Regulation of Investigatory Powers Act (RIP) in October 2000, giving employers limited rights of surveillance of their workforce, protesters claimed it was "a bleak day for privacy in Britain."

Yet many organisations have legitimate reasons for monitoring employees. These can range from simply wanting to be sure of the facts before accusing an employee of misconduct, to preventing corporate secrets from leaking out.

According to London-based security software company Peapod, 38% of large British companies already review email messages. A survey published by employment research specialist Industrial Relations Services puts the figure even higher. It suggests 77% of employers now routinely check to see what web sites employees are visiting, with emails being monitored by 55% of employers. Much of the time, their motives for monitoring employee activity are clear and valid.

Market analyst IDC reports that companies can lose up to £3 million a year in wasted time and bandwidth from employees surfing the web. And a study conducted by Professor Helen Petric of the University of Hertfordshire found that just 1.8% of employee respondents claimed to use email solely for legitimate company business.

Steve Donovan, a director of UK-based voice and data systems integration specialists, Armstrong Communications, freely admits to monitoring what his workforce is doing on the Internet. He says he has to know what is happening online to protect his business.

"Do I spend 90% of my time looking at my PC, checking up on my staff? No, I'm too busy," he maintains. "But if I want to know if I've got a problem with a member of my staff, it means I can go back and check what they were doing online. If I need to discipline someone, I need to know all the facts if I'm going to do it competently."

"There is increasing evidence that employers are monitoring without complying with the provisions of the code."

More serious than simple time-wasting, though, are security threats. With two-thirds of organisations in the UK having suffered virus, worm, or 'Trojan'-related problems over the past year, security is about protecting both employer and employee, says Jonathan Tait, European marketing manager at security software vendor, Content Technologies, which was recently acquired by rival Baltimore Technologies. "[Security software] protects the company's name and its brand, and protects it from ending up in court," he says. "We're not monitoring what people are doing. We're scanning for specific threats within emails and Internet access."

For one thing, employers are legally liable for what is published by their employees. This is why many businesses put a disclaimer at the bottom of emails. Email is a written communication, and is subject to the laws of libel. "It is also worth bearing in mind that emails often contain copyright information," says David Shepherd, editor of the Industrial Relations Services' *Employment Trends* bulletin, "and also that email is as secure as a postcard: stored on a server, and constantly misrouted."

The legislative framework

THERE is a fine balance between protecting a company's assets and ensuring some level of privacy and confidentiality for its employees. The situation is not aided by conflicting legislation that relates to email and Internet monitoring.

"Legislation surrounding anything to do with the Internet is in its infancy, because the Internet is in its infancy," says Tom Fawcett, security analyst at Frost & Sullivan. In the UK, for example, the Regulation of Investigatory Powers Act allows employers "routine access" to messages to check whether they are business-related, but under the proviso that companies make "all reasonable efforts" to inform staff and outside recipients of messages that they may be monitored.

However, the Act also allows employers to monitor staff phone calls, emails and Internet activities without consent and for a wide range of reasons. In contrast, the new Human Rights and Data Protection Acts give individuals the right to privacy at work, with the Data Protection Act threatening employers guilty of blanket snooping with enforcement action and unlimited fines if they read private emails.

Draft guidelines issued by the Data Protection Commissioner Elizabeth France also question whether blanket monitoring can be justified and stress that employees have a right to work without constantly being monitored. According to France, "There is increasing evidence that employers are undertaking monitoring without complying with the provisions of the code."

The effects of pan-European legislation are equally uncertain. A 1997 EU directive requires member states to protect the confidentiality of communications (phone calls, faxes, email and Internet), although interception is allowed. The jury is still out on the implications of the Human Rights Act for companies.

"It is not a detailed act," says Graham Titterington, senior analyst at Ovum Research. "Rather it is a sort of legal framework in which other legislation is viewed. It doesn't lay down the law, but may cause other laws to be regarded as void."

Trade unions are more bullish, saying they will use the Act to challenge rules on employee monitoring and court cases challenging the RIP bill are expected in the near future. "The data protection legislation may be something to watch more closely because that at least is specific," says Titterington. "Employees could argue that it is a piece of legislation that makes certain snooping activities illegal."

Two years ago, the European Court of Human Rights (ECHR) ruled that workers have a reasonable expectation of privacy in making and receiving calls at work. Some companies argue that because they own the computer resources on which email messages are transmitted, they should have unconditional right to control and monitor the contents of those messages. However, the ECHR is clear that ownership does not permit surveillance.

"Although the actual legal status of employers monitoring emails is still uncertain, the pendulum has obviously swung in favour of monitoring," adds Titterington. And Fawcett suggests that, "there are going to be cases where various issues are disputed in a court of law. Company policy will then have to follow the outcomes of such cases."

EMAIL JOKERS

When investment management company Gartmore was bought by the NatWest, its new parent company merged it with NatWest Investment and the merging of the two companies' IT systems gave all of Gartmore's employees Internet access.

Initially, groupware infrastructure manager Trevor Palmer believed the biggest threat would come from viruses. But the first problem came from another company about a joke it had received by email from a member of staff at Gartmore. After an investigation, Palmer discovered that the email was a personal message that had been sent to the right company – but the wrong person.

Palmer realised that unmonitored emails could quickly damage Gartmore's reputation. Palmer says the company has received two main benefits from installing an email monitoring system, Mimesweeper from Irish company, Baltimore Technologies. "Every email that goes out is the same quality as if it was a letter on company-headed paper. And the queuing time of business mails has been cut down: the whole system is much quicker."

Since staff are made aware the email system is a business tool, Palmer maintains, there are few complaints about email being monitored. "Content security is about being responsible for your company's data and, as a result, taking the security policy to the heart of corporate strategy."

However, it is unwise to rely on monitoring systems as a panacea for improper use of the Internet or email, if they are not sophisticated enough or if physical security is not great. Peter Norbury, employment specialist at law firm Eversheds, acted for a senior executive who was being undermined by emails sent out in her name by a subordinate.

"They didn't turn up on the email monitoring system because they were in a sort of code. These people know what they are doing. They use innocuous words." She found out about it because a colleague showed her a circular adding: "This doesn't sound like you."

Similarly, a solicitor was almost fired because his company's monitoring system had detected he was visiting web sites with at least 70% flesh-tone images – porn sites, it suggested. A search of the log revealed he had in fact been visiting the web site of well-known pink-coloured newspaper, the *Financial Times*.

Even the police have had problems with monitoring employees. Sergeant Gurpal Singh Virdi was suspended by London's Metropolitan Police after being accused of sending racist hate mail to ethnic minority colleagues at Ealing police station in West London.

The Complaints Investigation Bureau of the Metropolitan Police investigated Virdi, and officers discovered someone using his log-on had typed the first batch of letters. A second set had been printed off by someone using a different password – but from a terminal close to where he worked.

However, he was vindicated in August 2000 when an industrial tribunal cleared him, saying there was no evidence he had sent the mail. Indeed, the racist messages were probably never even in the computer printouts studied by the police, according to the tribunal. Had the logs been more detailed or physical security greater, Virdi might well never have been accused, sparing the Met a damages suit amounting to £150,000 as well as legal costs and bad publicity.

Dismissal for inappropriate use of a company's systems is, however, becoming

Court is in session

DO employees dismissed for email or Internet abuse have a right of appeal? Rupert Beverley and David Pennington thought so, after they were sacked from Huddersfield, UK-based Holset Engineering for forwarding smutty emails to colleagues.

The answer largely depends on whether or not their employer has a clear policy on monitoring which is communicated to their workforce. Pennington and Beverley had circulated jokes by email among a group of 40 willing employees at the company, but one email went astray and landed in the in-box of a colleague who did not share their sense of humour. He complained, and the company launched an investigation. After surveillance, Beverley and Pennington were sacked for being the ringleaders and forwarding more emails than anybody else.

An industrial tribunal unanimously rejected their claim for unfair dismissal. It found the company was perfectly within its rights to sack them not only for sending the emails, but also for the amount of time wasted in the process. The biggest mark in the company's favour was that it had a clear policy stating precisely what was acceptable material for inclusion in emails.

In contrast, in 1999, a college secretary claimed her manager put her under surveillance, monitoring her emails, Internet use and the length of her telephone calls. She says the manager even contacted people she phoned to check what the call was about and who they were. The college said checking up on staff was reasonable, but failed to produce a policy that detailed when and how managers could snoop on their staff. She lodged a complaint of harassment and, with the support of civil rights organisation Liberty, her case, which pre-dates the Regulation of Investigatory Powers Act of 2000, is being taken to the European Court of Human Rights.

"Email was intended to be a confidential communication between two individuals, whether on company business or not."

an increasingly common recourse for employers. In 1999, automotive repair company Kwik-Fit sacked two workers who were having an affair after their erotic emails were intercepted by management.

In September 2000, mobile phone company Orange sacked more than 45 members of staff for downloading pornographic images from the Internet and sending them through the Internet email system.

DISCIPLINARY ACTION

And in December 2000, it was announced that Bradley Chait, a lawyer at London law firm Norton Rose, was to face disciplinary action after he forwarded an email from his girlfriend Claire Swire, describing a sex act, to six of his friends.

Unfortunately for Chait, the email did not stop with his friends, but was passed on to an ever-widening circle of acquaintances, eventually reaching over a million people, and passing through the headquarters of organisations such as merchant bank JP Morgan and consumer goods multinational Unilever.

It is important, however, to distinguish between an employer's right to restrict employee Internet usage and blatant prying into supposedly confidential emails – a distinction that is made difficult by the complex web of legislation surrounding employee monitoring (see box, *The legislative framework*).

"I don't think there's been any doubt about an employer's right to block access to certain web sites or to control the use of the Internet from the workplace," says Graham Titterington, senior analyst at Ovum Research. "The main issues here are a waste of time and resources, and a wish not to have anything around that's not consistent with the tone of the organisation."

As well as using tools to dynamically monitor a web site for salacious content by looking for keywords and colour tone, some companies have gone a step further.

'Web bugs' hide computer codes behind images only a pixel in size on the computer screen to gather information about web surfing habits. Effectively, an invisible dot on the screen can watch every move a surfer makes, collecting information on the sites being visited as well as details of the computer being used.

Such sophisticated prying should be the last resort and not routine, argues Titterington. "Email was intended to be a confidential communication between two individuals, whether on company business or not," he says. "What we're seeing is not just the interception or prevention of transmission, but the opening of the contents." If the risk to the business through email is no greater than the risk of the telephone, it makes no sense to implement monitoring measures, he argues.

Titterington knows of one blue chip company that bans all external email, allegedly to protect itself against the risk of viruses. But the true motive behind the ban, he says, is a concern that employees may make an offer that becomes legally binding on the company.

"Employers have the right to withdraw the facility for sending personal email by means of blocking addresses," he says. "Looking into the contents of what is supposed to be a confidential communication is not acceptable. As for communications containing harassment or the racial vilification of other employees, you don't need to snoop on that as the receiver can complain. And once it's received, the email is their property."

Internet security should be a core business issue, but despite cases where people's rights have been infringed, two-thirds of companies either have no email and Internet policy, or don't enforce it.

The majority of company directors have little awareness of their 'cyberliability' for libel, copyright infringement, breach of confidence, negligent virus transmission, inadvertent contracts and computer hacking, according to the Integralis Group, which provides information and network security systems in the US and Europe.

"What it comes down to is defining a policy, communicating it and the reasons behind it to employees," says Tait of Content Technologies. "It's not about surveillance. It's not about opening up and reading every email." ⓘ

CONTACT
Article by Rob Buckley
Email: rbuckley@infoconomy.com