

Big Brother's Day at the Office

Mark Sanderson

With employee access to the Internet and external E-mail networks quickly becoming the norm, employers are becoming increasingly concerned with monitoring the activities of their employees at work. Figures show that 84% of the most serious frauds are committed by employees[1]. After the case of *Morse v Future Reality* [2] employers are justified in worrying about their exposure to sexual or racial harassment claims as a result of the downloading of pornography or circulation of distasteful jokes by E-mail. Employers are also concerned with their potential liability for defamatory statements made on their E-mail networks.

Technology allowing employers to monitor every movement of their employees is readily available; tiny CCTV cameras can watch employees from air vents, every key stroke an employee makes can be logged by desktop software, E-mails can be intercepted and telephones can be tapped. However, employers who decide to monitor their employees must have regard to a recent wave of legislation and guidance which limits the scope for a Big Brother style approach.

Monitoring of Physical Activity

The use of CCTV to monitor employees is covered by the recently enacted Data Protection Act 1998 (DPA 98) because it involves the processing of information relating to individuals from which they can be identified. Therefore the employer, as the Data Controller (having control over the purposes for which the information is used) must adhere to the principles of the DPA 98 contained in schedule 1.

Covert behavioural monitoring will only be justified in very limited circumstances, according to the Draft Code of Practice Relating to the Use of Personal Data in the Employer/Employee Relationship. Such circumstances are where informing employees of the monitoring would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

This would apply only where specific criminal activity has been identified and the monitoring is for the purposes of gathering evidence. Importantly, the Draft Code recommends that any other information collected in the course of covert monitoring must be disregarded unless it relates to behaviour serious enough to constitute gross misconduct or criminal activity.

Therefore CCTV operations should not involve the random selection of employees for surveillance.

If the operations are directed at collecting sensitive personal data, the employer must satisfy one of the grounds for holding the data contained in Schedule 3 of the DPA 98 in addition to the schedule 1 principles. Sensitive personal data consists of data relating to racial or ethnic origin, political beliefs, religious or other beliefs of a similar nature, trade union membership, health, sexual life and commission, or alleged commission, of an offence.

One of the grounds of Schedule 3 is consent. However, if the operation is aimed at catching out a dishonest employee with the purpose of instigating dismissal proceedings then the employer may rely on ground 6 which covers information gathered in connection with existing or prospective legal proceedings and avoid the need for consent. However, the employer must have legal proceedings against a specific individual in mind.

In obtaining sensitive and non-sensitive personal data the employer must comply with all the principles. This means obtaining the CCTV footage fairly and lawfully; informing employees that CCTV monitoring is being used; using it only for a specific purpose; limiting the data to adequate and relevant data; not holding the footage for longer than necessary; the employer should inform employees of the CCTV operation, its purpose and of any likely recipients of the footage.

Under section 10 of the DPA 98 employees who are being monitored by CCTV have, in some circumstances, the right to require the employer to cease or not to begin the collection of footage if it will result in substantial and unwarranted damage or distress. An employee who objects, may have a claim for constructive dismissal for a breach of the implied duty of trust and confidence owed by the employer. It could be argued, however, that employees who are informed of the surveillance and do not object, may be taken to have waived their right to object.

Automated Decision Making

Employees' performance is often monitored through software designed to count the amount of time spent at a workstation or the number of keystrokes per minute. However, under the DPA 98, a data subject has the right to require that no decision is taken solely on the basis of the automated monitoring. The employer must safeguard the interests of the employee or applicant, for example, by informing them of the automated decision making and allowing them of a right of appeal.

Interception of Telecommunications

Until recently the law on this subject was not comprehensive. However, the Regulation of Investigatory Powers Act 2000 (RIPA) which came into force on the 24 October 2000 has added to the already heated privacy debate.

The situation pre-RIPA

The Interception of Communications Act 1985 (ICA 95) made it a criminal offence to intercept communications by using public telecommunications network unless there is a warrant in force or the interceptor believes that one of the parties to the communication consents. However, this only applied to telephone calls, faxes and E-mails on public networks and provides no protection to employees who use private telecommunications systems.

The class licences for private networks usually require the licensee to make 'every reasonable effort' to inform users that calls may be recorded. However, there is no effective remedy to back this condition up. Neither do the licences cover E-mail or fax, as they are not live speech communications. If the employee manages to find out about the interceptions in the first place, he may again be able to rely upon a breach of duty of trust and confidence.

New Legislation

Under RIPA employers are more restricted in their interception of communications which take place on private and public networks as long as the private network is connected to the public network.

On a public network, it is an offence to intercept any communication without lawful authority. Lawful authority can be obtained by the issue of a warrant under RIPA or under the Lawful Business Practice Regulations[3] which came into force on the same day.

On a private network, it is an offence for someone who does not control the system to intercept communications. However, an employer who controls the system will be open to a civil action from either party to the communication if they intercept communications without either reasonable belief that both parties of the communication consent to the interception; or lawful authority.

Under the Lawful Business Practice Regulations (the Regulations) interception is 'authorised' for the purposes of

RIPA in the following circumstances: Monitoring business communications to ascertain whether business standards and procedures are being complied with and establishing the existence of facts; national security; preventing or detecting of crime; detecting unauthorised use; providing evidence of facts or ascertaining compliance with relevant procedures to the business; charitable help lines.

These provisions are designed to strike a balance between the privacy of individuals and the need for businesses to get the maximum benefit from their investment in telecommunications technology.

However, the interception must be in connection with the employer's business; and on a telecommunications system provided wholly or partly in connection with the business.

If the employer cannot claim the benefit of one of the above sets of circumstances then it must obtain a warrant in order to intercept without informing users.

Under the Regulations employers must make all reasonable efforts to inform employees or other callers of the possibility of interception or have grounds to believe that callers are aware of the possibility.

However, merely informing employees of the fact of interception may not be enough. Additional Government guidance[4] was circulated in March 1999 stating that an employee who has been informed of the possibility of interception no longer has an expectation of privacy. Although the same guidance warns that it is not reasonable to expect that employees will never be contacted for domestic reasons or have reasons to make personal calls.

Employers should have an adequate policy in place which describes in which circumstances private calls and E-mails will be tolerated and the sanctions for non-compliance. This will help to clarify where an employee has a legitimate expectation of privacy.

Having a clear and fair policy on use of the telephone, Internet and E-mail at work is advisable in the light of the *Dunn and Kwik Fit* [5] cases where failure to implement an IT policy lead to the

conclusion by the Employment Tribunal that a summary dismissal was unfair. The best way to approach the issue of such a policy is to publicise it and make it clear that non-compliance will lead to disciplinary action.

Where RIPA does not apply, the DPA 98 and Codes of Practice will still apply to the interception of telecommunications and collection of personal data. The provisions outlined above for CCTV are applicable to the collection of personal data by all other methods.

Human Rights

The Human Rights Act 1998 (HRA 98) came into force in October 2000. It incorporates the rights enshrined in the European Convention of Human Rights (ECHR) into UK Law. The main provision of the HRA 98 is that all public bodies will be required to act in accordance with the ECHR.

Of particular relevance here is Article 8 of the ECHR which gives every person "the right to respect for his private life, his home and his correspondence".

Employers who are public bodies will have to bear this in mind when undertaking surveillance of their employees. However, since the Courts could begin to apply domestic law in a way which is compatible with the ECHR, employers in the private sector could also have their human rights credentials subjected to scrutiny if they are taken to court. Whether the Courts will take such an approach is still a theoretical possibility and it remains to be seen how they will react. One limitation of the HRA 98 is that actions can only be brought against public bodies and in order to invoke the HRA 98 potential claimants must find another legal basis for their claim against a private body.

Many of the surveillance techniques outlined here could be abused in a way that invades employees' privacy. An employer must therefore be very careful to comply with any domestic legislation and any Code of Practices as this will weigh in an employer's favour. The DPA 98 itself is based on an EC directive

whose object is specified as being to align national laws with the protection of the principles Article 8 of the ECHR.

Cases involving Human Rights arguments are likely to be decided on a case by case basis. Employers should take care in weighing up other interests against their employees' privacy and be careful to act proportionately. For example, economic considerations are less likely to justify invasions of privacy than protecting the legitimate privacy interests of third parties. If employers do find it necessary to limit the privacy enjoyed by their employees in favour of competing interests, the least restrictive means possible should be used.

Article 8(2) of the ECHR provides for legitimate aims which an employer may pursue without breaching Article 8. These are national security; public safety; economic well being of the country; prevention of disorder and crime; protection of the rights and freedoms of others.

However, there will always be a careful balancing act between the interests of society in general and the privacy of the individual.

One recent example of an European Court of Human Rights decision in relation to Article 8 is *Aural Rotaru v Romania* [6]. In this case, the holding of a secret file containing inaccurate information that the applicant was a member of a political movement amounted to an interference of his right to respect for his privacy and family life. The interference was not made under a legitimate aim under Article 8(2). Therefore, the holding of the secret file was in breach of Article 8.

Employers who monitor their employees must bring their activities within the new legislative framework and conduct their activities with a respect for the privacy of their employees. The visions of a Big Brother society have become a technical possibility. However, the protection afforded to individuals is now catching up with the pace of technological advances.

About the author

Mark Sanderson is a Senior Associate at Masons Solicitors an international firm specialising in the legal issues affecting the IT industry.

References

- [1] PPRU Study Report "The uses and misuses of personal data in employer employee relationships" January 1999
- [2] *Morse v Future Reality Ltd* — ET Case No 54571/95
- [3] The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- [4] Home Office Circular 15/1999
- [5] *Dunn v IBM UK* — ET Case no. 2305087/97
- [6] *Aural Rotaru v Romania*, European Court of Human Rights Application No. 00028341/95, 4 May 2000

Freedom Without Compromise: Creating a Secure Environment on the Move

Guy Singh, Baltimore Technologies

E-commerce has already begun to revolutionize the way we work, shop and do business. But the transformation to a digital economy will not be complete until it encompasses mobile commerce. Although still a relatively new capability, M-commerce has the potential to create a whole new service sector, new business models and new avenues for customer service. This has been said about E-commerce, of course, though the difference is that by taking E-commerce away from the desktop, M-commerce will be much more pervasive than E-commerce as we know it today. A combination of the two most explosive technologies of the last ten years — the World Wide Web and wireless communications — M-commerce is widely cited as a huge opportunity for businesses across the globe.

There are currently over 500 million wireless subscribers and by 2003 there will be over a billion. Analysts at Ovum have predicted that the number of

Internet-enabled mobile devices, including smart phones and networked palmtop computers, will exceed the number of PCs by 2003. The amount spent on

M-commerce services will rise to more than \$200 billion in 2005, it predicts.

However, many analysts believe that M-commerce today is still at the very earliest stage of development, and that it will not reach full viability for another three years. To unlock the potential of M-commerce, there are fundamental security issues that must be solved. E-business security breaches in the banking and utilities sectors have damaged consumers' confidence in making transactions over the Internet. Such breaches — and the arrival of digital signature legislation around the globe — have highlighted the need for the business community to prioritize E-security. Reputable companies must provide their customers with a secure framework for E-business over a solid, wired infrastructure. Industry must allay the fears of businesses and consumers so that trusted, mutual relationships can be forged.

M-commerce fundamentals

In Europe, the WAP (Wireless Application Protocol) standard provides