Surveillance, Monitoring and the Law

PLEASE NOTE THAT THIS ARTICLE WAS WRITTEN IN FEBRUARY 2001. CERTAIN ASPECTS OF THE DATA PROTECTION ACT HAVE NOW CHANGED IN THE LIGHT OF THE DURANT JUDGEMENT AND THE EMPLOYEMENT PRACTICES DATA PROTECION CODE PART 3.

Delivering services electronically is the current mantra of local government. Consequently an increasing number of council employees, especially in the revenues and benefits sector, now have access to Internet and e-mail facilities. However just like there are massive benefits to these technologies if used responsibly, the legal risks to the organisation are also greatly multiplied. Many cases have now come before the courts involving staff claims of harassment, defamation etc. by means of the Internet and e-mail in the workplace. In June 45 Orange employees were sacked for distributing pornography downloaded from the Internet.

Software and hardware is available which allow everything from eavesdropping on staff phone calls to filtering their e mails and logging which web sites they visit. But misuse is not the only reason why managers may want to know what staff are doing with the technology at their disposal.. They may want to access staff e mails when they are absent or wish to listen in/record telephone calls to see if training is effective or to check adherence to regulatory rules. The question arises as to whether this “snooping” is lawful? The answer lies in examining four recent pieces of legislation:

The Regulation of Investigatory Powers Act 2000

The Regulation of Investigatory Powers Act 2000 (RIP Act) repeals the Interception of Communications Act 1985 and establishes a new legal framework for the interception of communications. Previously there was nothing preventing an employer from carrying out surveillance on internal telephone or e mail systems The Act ensures that the UK's interception regime is compliant with the Telecommunications Data Protection Directive (97/66/EC). It covers all types of electronic communication made by means of a public telecoms network including, for example, fax and email. The requirement also extends to communications on private networks which will also travel or have also travelled on a public network.

The RIP Act creates a tort of unlawful interception on a private telecommunication system by the operator of that system i.e. any organisation that carries out interception of any communication on its own system can potentially be sued by the users, not just the employees. However such interception is authorised where the interceptor has reasonable grounds to believe that both the sender and intended recipient have consented to the interception. Thus, reading the Act in isolation, employers may only intercept communications if there are reasonable grounds to believe that the users have consented. If they intercept unlawfully, the sender or recipient of the communication may be able to obtain an injunction or sue for damages. The Secretary of State can make Regulations authorising businesses to intercept on their own systems without consent for certain purposes. This power has been recently used to enact the following regulations.

The Telecommunications (Lawful Business Practice) (Interception of communications) Regulations 2000

These Regulations came into force on 24th October 2000. Their purpose is to give businesses a lawful basis for the interception of business communications without the users' consent for a range of purposes. The Regulations will cover all types of communications including those that are Internet based , by fax and by email.

The Regulations allow businesses, government department, and any public authority to monitor or record communications to:

(a) Establish the existence of facts
(This will allow interception for purposes such as audit, dispute resolution etc.)

(b) Ascertain compliance with practices or procedures (regulatory or self regulatory).

(c) Monitor standards of service and staff training

(d) Safeguard national security

(e) Detect and prevent crime
(e.g. fraud or corruption)

(f) Prevent or detect the unauthorised use of a telecommunications system.
(This will allow interception for detecting the unauthorised use/misuse of an e mail/internet system by employees.)

(g) Maintain the effective operation of the system
(e.g. to protect the network against viruses or hackers.)

Employers may also monitor but not record communications for the purposes of establishing whether or not the communication relates to the business. This allows, according to the DTI, the opening of an employee's e mail account whilst he is on holiday. Furthermore monitoring (but not recording) of communications to helplines providing confidential counselling and support services free of charge on an anonymous basis is allowed.

In all of the above cases the interceptor is required to make all reasonable efforts to inform correspondents that the communication may be intercepted. This may be easy to do in respect of telephone calls but what about faxes and e mail? It is suggested that if these too are the subject of monitoring managers should add some standard wording to outgoing faxes and emails. One further point to note is that the regulations only apply to systems that have been provided wholly or mainly for business use. Payphones or other facilities provided for private use are not covered.

The effect of the RIP Act and the Regulations is that, in future, organisations or managers which intercept on their own systems, will need to be sure that their actions are legally authorised either through getting consent from the users or through ensuring they fall into one of the above categories. The DTI intends to review the Regulations after twelve months from their entry into force or, if later, after the adoption of the revised Telecoms Data Protection Directive proposed by the EU Commission.

The Data Protection Act 1998

Any interception which involves obtaining, recording or otherwise processing personal data by means of automated equipment (for example recording calls or filtering email contents) also falls within the scope of the Data Protection Act 1998. So too does the holding or processing of personal data after the interception has taken place. The Act came into force on 1st March. It gives increased rights of access to the subjects and also places heavier obligations on those processing the data. Amongst other things, the Act requires the personal data to be processed fairly and lawfully and for the subject to be given access to it.

In addition the Data Protection Commissioner has issued a draft of a statutory code of practice entitled "The use of Personal data in employer employee relationships". This can be downloaded from her website(www.dataprotection.gov.uk). It lays down strict rules for the monitoring of employees at work including the interception of communications. Unfortunately the draft Code, released before the final version of the Lawful Business Regulations, is much stricter and contains conflicting provisions. The Regulations allow access to the communications and consequently their content. However the Commissioner states in the Code that the contents of emails should not be monitored unless it is clear that the business objective could not be fulfilled through traffic monitoring i.e. looking at the source and recipient of email but not the content.

She goes on to state that where emails' contents are monitored it should not be the ones deleted but only the ones kept by the user. There are no such restrictions in the Regulations. The Commissioner states: "An employee has a right to expect a degree of trust from the employer and be given reasonable freedom to determine his or her actions without constantly being watched or asked to explain." It may be that this conflict is resolved only after litigation. It will be interesting to see if the Commissioner is pressured into softening her stance to monitoring in the final version of the Code. In the meantime it is suggested that managers think long and hard about the need for monitoring the contents of communications and what justification there is for it.

The Human Rights Act 1998

The legal waters have been further muddied by the influence of the European Convention on Human Rights, now incorporated into UK law as a result of the Human Rights Act 1998. This confers the right to privacy on individuals not just in the home but also in the workplace (article 8). In Halford v UK Government the European Court of Human Rights found that the secret interception of calls made by Ms Halford from her office amounted to an unjustifiable interference with her right to respect for her privacy and correspondence.

The Lawful Business Regulations are designed to allow business to check on employees without fear of breaching their right of privacy. Whether or not they do this is a matter of great debate. Some argue that the Government's decision not to force employers to obtain prior agreement from senders and recipients for most monitoring (as was the case in the draft regulations), has turned the tide in favour of employers. They argue that the Regulations give businesses almost carte blanche powers to monitor staff in the workplace and so are incompatible with the Human Rights Act. The Trades Union Congress has stated that it will challenge the new regulations in the courts on this basis.

Practical Steps

Managers who wish to carry out surveillance must at least ensure that they have justification under one of the categories in the Lawful Business Regulations. Best practice requires them to seek the consent of users wherever possible. The best way to do this in respect of staff is to formally introduce a workplace policy which is read by all setting out exactly when and how surveillance will take place. This does not need to be specific to the revenues/benefits service. The Councils corporate policy will be adequate as long as it covers the following points:

- It should be emphasised that all modes of communication are essentially business tools.
- Personal use of communications should be addresses and employees must be told not to expect privacy.
- The precise nature of surveillance must be explained and when it will be carried out.
- The policy must have disciplinary sanctions within it
- It should be brought to the attention of all employees through the intranet, staff handbook or posters.

Surveillance of staff communications is a very emotive issue and one which needs to be handled sensitively. Managers need to be open and honest and have a degree of trust in their staff. A policy which fully explains matters and which is passed after consultation with staff representatives will go a long way to ensuring that managers are not accused of having a “snoopers' charter”.

Ibrahim Hasan, formerly a local authority solicitor, is now a writer and adviser on information law and privacy issues with Act Now Training and IBA Solicitors

Email:ih@informationlaw.org.uk