

## WHEN BIG BROTHER IS KEEPING WATCH

**After extensive consultation with business and a delay of two years, the Information Commissioner has published Part 3 of the Employee Practices Data Protection Code. The code deals with whether companies can monitor employee telephone calls, internet usage and emails in the workplace.**

Part 3 of the Employee Practices Data Protection Code does not set new law but provides best practice guidance in the context of the Data Protection Act. The code contains benchmarks the Information Commissioner can use to take action against employers that intrude on employee privacy via secret filming, taping or monitoring of their communications.

The courts and employment tribunals are likely to take the code seriously, and recent court cases such as the Naomi Campbell privacy case suggest the courts are already guided by the Commissioner's views.

### Best practice

The act doesn't generally prevent monitoring, but sets out principles that apply when it is carried out. In short, any adverse impact of monitoring on workers' privacy must be justified by its benefit to the employer and/or others.

Employees should be aware of the nature, extent and reasons for any monitoring before it is undertaken, unless covert monitoring is undertaken, in which case the employer should involve the police.

The Commissioner's guidance to employers suggests:

- Consider why you want to carry out the monitoring. This might

involve identifying a problem you are trying to solve; for example, theft in the workplace.

- Once you are clear about the purpose, satisfy yourself the particular monitoring arrangement is justified by real benefits that will be delivered. The code suggests employers undertake an 'impact assessment' for every monitoring action undertaken.

- Remember, it is generally considered intrusive to monitor employees. They have legitimate expectations that they can keep their personal lives private and workers are entitled to a degree of privacy in the workplace.

- Ensure your employees are aware they are being monitored and why. Inform them using a noticeboard or signage in areas where monitoring is taking place. You could send an email telling them about the monitoring.

Employee awareness will influence their expectations and create an environment of trust.

- If monitoring is to be used to enforce company rules and standards, make sure employees know what these are; for example, are your workers clear on company policy toward pornography, use of private emails, making private telephone calls, etc?

- Only use information obtained through monitoring for the purpose for which the monitoring was carried out, unless the monitoring leads to the discovery of an activity that no employer could reasonably be expected to ignore; for example, breaches of health and safety rules that put other workers at risk.

- Keep the information you obtain through monitoring secure. This might mean only allowing one or

two people to access it.

Companies should ensure they don't keep the information longer than necessary and are advised to delete information once disciplinary action against a worker is over.

### Email monitoring

The code states that employers should be particularly careful when monitoring emails. Employers should avoid opening emails, especially those which clearly show they are private or personal. Employers should confine monitoring to the message's address and subject field.

This begs the question, 'What constitutes an exceptional circumstance as written in the code?' In other words, what are the instances where employers can *open* employee emails. The code doesn't address this question but hints at issues such as breaches of the law or company health and safety as mitigating factors.

Gary Brooks from law firm Berwin Leighton Paisner says: "Exceptional circumstances would, in my view, include situations where the employer has reasonable grounds for believing the employee is breaching internal policies on the use of email. It would also cover situations where the employer suspects the employee is breaching the terms of his employment contract; for example, where the employee is spending his work time carrying out unauthorised work for another business. Obviously, if the employer suspects the employee is engaged in criminal activity against it, then opening a personal email as part of an internal investigation is clearly justified."

### Employee rights

Workers have a legal right to access the information employers hold on them, including information obtained through monitoring.

Normally, employers must give an employee access to all information on them within 40 days of a request to do so, but information can be withheld if it is felt it could prejudice the detection of crime.

Employees should be allowed to make representations about the information gathered through monitoring where it might have an adverse impact on them. It may be that equipment or systems malfunction means the information obtained through monitoring is inaccurate or misleading. Information obtained from third parties may simply be wrong.

Brooks says that complying with the new code is about constantly communicating company policy to employees. "If companies have spent time drafting a computer use policy and have kept it under review, then those companies will be in a better position to defend their corner with the Information Commissioner or at an employment tribunal," he says.

*Tom Berry*

*A wide range of Briefings can be found at [www.financialdirector.co.uk/briefing](http://www.financialdirector.co.uk/briefing)*

### Useful links

- A copy of the **Employment Practices Data Protection Code and advice on implementing data protection legislation can be found on the 'guidance and other publications' section of [www.dataprotection.gov.uk](http://www.dataprotection.gov.uk)**

- **Information Commissioner, [www.informationcommissioner.gov.uk](http://www.informationcommissioner.gov.uk)**

- **Gary Brooks, Berwin Leighton Paisner, [gary.brooks@blplaw.com](mailto:gary.brooks@blplaw.com)**