INTERACTIVE SESSION: ORGANIZATIONS

MONITORING IN THE WORKPLACE

There may be only 11 players on the pitch during a match, but the Blackburn Rovers Football Club in the UK employs more than 800 people. As with any modern organization, computers are at the heart of running an efficient business. Most of the club's computers are housed with the administration department at the Ewood Park office, but others can be found at the club's training center and soccer academy.

The club decided to install a software product called Spector 360, which it obtained from the Manchester-based company Snapguard. According to Snapguard's sales literature, the product enables company-wide monitoring of employee PC and Internet usage. Previously, the club had tried to introduce an acceptable use policy (AUP), but initial discussions with employees stalled, and the policy was never implemented. Early trials of Spector 360 showed that some employees were abusing the easygoing nature of the workplace to spend most of their day surfing the Web, using social networking sites, and taking up a huge amount of bandwidth for downloads.

Before officially implementing the monitoring software, the AUP was resurrected. It was sent out as an e-mail attachment and added to the staff handbook. The policy was also made part of the terms and conditions of employment. Understandably, some employees were annoyed at the concept of being watched, but the software was installed anyway. According to Ben Hayler, senior systems administrator at Blackburn Rovers, Spector 360 has definitely restored order, increasing productivity and reducing activity on non-business apps.

Reports provided by Spector 360 can show managers the following: excessive use of Facebook, Twitter, and other social networking sites; visits to adult sites or shopping sites; use of chat services; the printing or saving of confidential information; and staff login and logout times. Managers can also use the software to drill-down to look at patterns of usage, generate screen snapshots, or even log individual keystrokes.

The software can also be used to benefit employees. For example, because it can log exactly what an employee is doing, the system can help in staff training and troubleshooting, because it is easy to track exactly what caused a particular problem to occur.

Another important benefit of the software is that it helps the club to stay compliant with the Payment Card Industry (PCI) Data Security Standard. PCI standards require access to credit card information. As Spector 360 tracks and records all data to do with credit card transactions, the information can be easily recovered.

However, what is the wider view of the monitoring of employees in the workplace? According to the Citizens Advice Bureau (a free information and advice service for UK residents), the following are some of the ways that employers monitor their employees in the workplace: recording the workplace on CCTV cameras; opening mail or e-mail; using automated software to check e-mail; checking telephone logs or recording telephone calls; checking logs of Web sites visited; videoing outside the workplace; getting information from credit reference agencies; and collecting information from point-of-sale terminals.

Although this list may look formidable, there is no argument that the employer has a right to ensure that his or her employees are behaving in a manner that is not illegal or harmful to the company. However, under UK data protection law the employer must ensure that the monitoring is justified and take into account any negative effects the monitoring may have on staff. Monitoring for the sake of it is not allowed. Secret monitoring without employees' knowledge is usually illegal.

In a case that went before the European Court of Human Rights in 2007 (Copeland v the United Kingdom), Ms. Copeland, who was an employee of Carmarthenshire College, claimed that her privacy had been violated. She was a personal assistant to the principal and also worked closely with the deputy principal, who instigated monitoring and analysis of her telephone bills, Web sites visited, and e-mail communication. The deputy principal wanted to determine whether Copeland was making excessive use of the college's services. The European Court ruled in her favor, stating that her personal Internet usage was deemed to be under the definitions of the Convention for the Protection of Rights, covered as "private life." Note that although this case came to the court in 2007, the monitoring took place in 1999, prior to the introduction into English and Welsh law of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) Regulations 2001, which seek to clarify regulations about the interception of communications.

The major fault of Carmarthenshire College was in not having a usage policy in place. Employers and employees should have an agreed-upon policy as part of the contract of employment that clarifies what is and is not acceptable computer usage in the workplace. The employer can then follow normal disciplinary procedures if an employee is using workplace equipment in a manner that is not permitted in the contract of employment.

Whatever the legal situation, it is clear where potential problems can occur in the workplace regarding information technology use. An e-mail, once sent, becomes a legally published document that can be produced as evidence in court cases involving issues of libel, breach of contract, and so on. Most businesses rely on their company data to keep ahead of the competition. Therefore, the loss, theft, or sabotage of data is potentially more dangerous than similar problems with hardware. If a stick is lost in a bar parking lot, replacing the hardware will cost a few dollars, but if it contains the company's confidential data, then its loss could put the company out of business!

Many companies place great focus on employee productivity. It is relatively easy to block access to certain sites (e.g., YouTube, Facebook, etc.), but a blanket blocking of such sites could cause problems if an employee has a legitimate need to access a site. In addition, should sites be blocked during lunch hour? In any case, blocking such sites on the desktop computer is becoming less of a guarantee of increased productivity nowadays (if it ever was), as more and more employees will just use their smartphones to access these sites anyway.

Sources: Information Commissioners Office, "Employment Practices Data Protection Code-Supplementary Guidance" (www.ico.gov.uk/upload/documents/library/data_protection/practical_application/coi_html/english/supplementary_guidance/monitoring_at_work_3.html, accessed October 25, 2010); "Spector 360 Helps Blackburn Rovers Show Red Card to PC and Internet Abuse," Snapguard (www.snapguard.co.uk/blackburn_fc.html, accessed October 25, 2010); "Citizens Advice Bureau Advice Guide, Basic Rights at Work," Adviceguide (www.adviceguide.org.uk/index/your_money/employment/basic_rights_at_work.htm, accessed October 25, 2010); "Employee Monitoring in the Workplace: What Constitutes 'Personal Data'?" Crowell and Moring (www.crowell.com/NewsEvents/ Newsletter.aspx?id = 654, accessed October 25, 2010).

Case contribued by Andy Jones, Staffordshire University.

CASE STUDY QUESTIONS

1. Do you consider the approach taken by Blackburn Rovers to be too strict on employees, too lenient, or just right?
2. Consider the five moral dimensions described in the text. Which are involved in the case of Copeland v. the United Kingdom?
3. Consider the following scenario. Your 14-year-old son attends a soccer academy. While there, he downloads unsuitable images, which he later sells to his friends. He would not have been able to download the images at home, because you have installed parental control software. Who is to blame for his indiscretion?
4. Why is the digital divide problem an ethical dilemma?