INTERACTIVE SESSION: MANAGEMENT

MONITORING EMPLOYEES ON NETWORKS: UNETHICAL OR GOOD BUSINESS?

The Internet has become an extremely valuable business tool, but it's also a huge distraction for workers on the job. Employees are wasting valuable company time by surfing inappropriate Web sites (Facebook, shopping, sports, etc.), sending and receiving personal email, talking to friends via online chat, and downloading videos and music. According to IT research firm Gartner Inc., non-work-related Internet surfing results in an estimated 40% productivity loss each year for American businesses. A recent Gallup Poll found that the average employee spends over 75 minutes per day using office computers for non-business related activity. That translates into an annual loss of $6,250 per year, per employee. An average mid-size company of 500 employees could be expected to lose $3.25 million in lost productivity due to Internet misuse.

Many companies have begun monitoring employee use of e-mail and the Internet, sometimes without their knowledge. Many tools are now available for this purpose, including SONAR, Spector CNE Investigator, iSafe, OsMonitor, IMonitor, Work Examiner, Net Spy, Activity Monitor, Mobistealth, and Spytech. These products enable companies to record online searches, monitor file downloads and uploads, record keystrokes, keep tabs on emails, create transcripts of chats, or take certain screenshots of images displayed on computer screens. Instant messaging, text messaging, and social media monitoring are also increasing. Although U.S. companies have the legal right to monitor employee Internet and e-mail activity while they are at work, is such monitoring unethical, or is it simply good business?

Managers worry about the loss of time and employee productivity when employees are focusing on personal rather than company business. Too much time on personal business translates into lost revenue. Some employees may even be billing time they spend pursuing personal interests online to clients, thus overcharging them.

If personal traffic on company networks is too high, it can also clog the company's network so that legitimate business work cannot be performed. Procter & Gamble (P&G) found that on an average day, employees were listening to 4,000 hours of music on Pandora and viewing 50,000 five-minute YouTube videos. These activities involved streaming huge quantities of data, which slowed down P&G's Internet connection.

When employees use e-mail or the Web (including social networks) at employer facilities or with employer equipment, anything they do, including anything illegal, carries the company's name. Therefore, the employer can be traced and held liable. Management in many firms fear that racist, sexually explicit, or other potentially offensive material accessed or traded by their employees could result in adverse publicity and even lawsuits for the firm. An estimated 27 percent of Fortune 500 organizations have had to defend themselves against claims of sexual harassment stemming from inappropriate email. Even if the company is found not to be liable, responding to lawsuits could run up huge legal bills. Symantec's 2011 Social Media Protection Flash Poll found that the average litigation cost for companies with social media incidents ran over $650,000.

Companies also fear leakage of confidential information and trade secrets through e-mail or social networks. Another survey conducted by the American Management Association and the ePolicy Institute found that 14 percent of the employees polled admitted they had sent confidential or potentially embarrassing company e-mails to outsiders.

U.S. companies have the legal right to monitor what employees are doing with company equipment during business hours. The question is whether electronic surveillance is an appropriate tool for maintaining an efficient and positive workplace. Some companies try to ban all personal activities on corporate networks—zero tolerance. Others block employee access to specific Web sites or social sites, closely monitor e-mail messages, or limit personal time on the Web.

For example, P&G blocks Netflix and has asked employees to limit their use of Pandora. It still allows some YouTube viewing, and is not blocking access to social networking sites because staff use them for digital marketing campaigns. Ajax Boiler in Santa Ana, California, uses software from SpectorSoft Corporation that records all the Web sites employees visit, time spent at each site, and all e-mails sent. Financial services and investment firm Wedbush Securities monitors the daily e-mails, instant messag-

ing, and social networking activity of its 1,000-plus employees. The firm's e-mail monitoring software flags certain types of messages and keywords within messages for further investigation.

A number of firms have fired employees who have stepped out of bounds. A Proofpoint survey found that one in five large U.S. companies fired an employee for violating e-mail policies in the past year. Among managers who fired employees for Internet misuse, the majority did so because the employees' e-mail contained sensitive, confidential, or embarrassing information.

No solution is problem-free, but many consultants believe companies should write corporate policies on employee e-mail, social media, and Web use. The policies should include explicit ground rules that state, by position or level, under what circumstances employees can use company facilities for e-mail, blogging, or Web surfing. The policies should also inform employees whether these activities are monitored and explain why.

IBM now has "social computing guidelines" that cover employee activity on sites such as Facebook and Twitter. The guidelines urge employees not to conceal their identities, to remember that they are personally responsible for what they publish, and to refrain from discussing controversial topics that are not related to their IBM role.

The rules should be tailored to specific business needs and organizational cultures. For example, investment firms will need to allow many of their employees access to other investment sites. A company dependent on widespread information sharing, innovation, and independence could very well find that monitoring creates more problems than it solves.

Sources: "Should Companies Monitor Their Employees' Social Media?" *Wall Street Journal*, May 11, 2014; Rhodri Marsden, "Workplace monitoring mania may be risky business," Brisbane Times, March 30, 2014; Donna Iadipaolo, "Invading Your Privacy Is Now the Norm in the Workplace," Philly.com, April 28, 2014; "Office Slacker Stats," www.staffmonitoring.com, accessed May 1, 2014; "Office Productivity Loss," Staffmonitoring.com, accessed May 1, 2014; "Workplace Privacy and Employee Monitoring," Privacy Rights Clearinghouse, June 2013; Samuel Greengard, "How Smartphone Addiction Hurts Productivity," *CIO Insight*, March 11, 2013; Emily Glazer, "P&G Curbs Employees' Internet Use," *The Wall Street Journal*, April 4, 2012; and David L. Barron, "Social Media: Frontier for Employee Disputes," Baseline, January 19, 2012.

CASE STUDY QUESTIONS

1. Should managers monitor employee e-mail and Internet usage? Why or why not?
2. Describe an effective e-mail and Web use policy for a company.
3. Should managers inform employees that their Web behavior is being monitored? Or should managers monitor secretly? Why or why not?

other and had to be managed separately by the information systems department. Now, however, firms are able to merge disparate communications modes into a single universally accessible service using unified communications technology. **Unified communications** integrates disparate channels for voice communications, data communications, instant messaging, e-mail, and electronic conferencing into a single experience where users can seamlessly switch back and forth between different communication modes. Presence technology shows whether a person is available to receive a call. Companies will need to examine how work flows and business processes will be altered by this technology in order to gauge its value.

CenterPoint Properties, a major Chicago area industrial real estate company, used unified communications technology to create collaborative Web sites for each of its real estate deals. Each Web site provides a single point for accessing structured and unstructured data. Integrated presence technology lets team members e-mail, instant message, call, or videoconference with one click.