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 websites (Facebook, shopping, sports, etc.), sending and receiving personal email, texting to friends, and downloading videos and music. According to a survey by International Data Corp (IDC), 30 to 40 percent of Internet access is spent on non–work-related browsing, and a staggering 60 percent of all online purchases are made during working hours. UK-based employment site MyJobGroup.co.uk surveyed 1,000 British workers and found that almost 6 percent of them spent over an hour a day using social media of some kind, including *Facebook*. This is roughly one-eighth of their workday. By extension, about 2 million of Britain's 34-million-person workforce likely were doing the same, costing the British economy about 14 billion pounds in lost productivity.

Many companies have begun monitoring employee use of email and the Internet, sometimes without their knowledge. Many tools are now available for this purpose from vendors such as Veriato OsMonitor, Work Examiner, 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.

Microsoft Corporation collects and analyzes data on the frequency of chats, emails, and meetings between its staff and clients using its own Office 365 services to measure employee productivity, management effectiveness, and work-life balance. Tracking email, chats, and calendar appointments can show how employees spend an average of 20 hours of their work time each week. The company only allows managers to look at groups of five or more workers.

Microsoft sales team members have received personalized dashboards that show how they spend their time, but this information is shielded from managers. The dashboards offers recommendations on how to build out networks of contacts and spend more time with customers rather than in internal meetings.

Microsoft also sells workplace analytics software to other companies, such as Macy's Inc., which analyzed data on staff work-life balance by measuring how many hours employees spent sending emails and logged in online outside of business hours. Mortgage giant Freddie Mac used Microsoft's tools to gauge how much time workers spent in meetings and try to determine whether some of those gatherings were redundant.

Although U.S. companies have the legal right to monitor employee Internet and email 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. GMI Insurance Services, which serves the U.S. transportation industry, found that employees were downloading a great deal of music and streaming video and storing the files on company servers. GMI's server backup space was being eaten up.

When employees use email 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. Even if the company is found not to be liable, responding to lawsuits could run up huge legal bills. Companies also fear leakage of confidential information and trade secrets through email or social networks. 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 websites or social sites, closely monitor email messages, or limit personal time on the web.

Should all employees be monitored while working? Not necessarily. Not every workforce, workplace, or work culture and environment is a candidate for electronic surveillance. The decision depends on the company and the work environment an employer wants to create. A major concern of some employers is the potential damage to a work culture that fosters trust, employee commitment, and motivation. Electronic surveillance of employees could prove highly counterproductive in such an environment.

No solution is problem-free, but many consultants believe companies should write corporate policies on employee email, social media, and Internet use. Many workers are unaware that employers have the right to monitor and collect data about them. The policies should include explicit ground rules that state, by position or level, under what circumstances employees can use company facilities for email, blogging, or web surfing. The policies should also inform employees whether these activities are monitored and explain why.

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: "How Do Employers Monitor Internet Usage at Work?" wisegeek.com, accessed March 1, 2020; Sarah Krouse, "The New Ways Your Boss Is Spying on You," *Wall Street Journal,* July 19, 2019; www.privacyrights.org, accessed February 15, 2020; and Susan M. Heathfield, "Surfing the Web at Work," thebalanecareers.com, November 25, 2019.

CASE STUDY QUESTIONS

1. Should managers monitor employee email and Internet usage? Why or why not?
2. Describe an effective email 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?

the economies of scale and management facilities of large networks, such as the Internet (see Figure 7.10). A VPN provides your firm with secure, encrypted communications at a much lower cost than the same capabilities offered by traditional non-Internet providers that use their private networks to secure communications. VPNs also provide a network infrastructure for combining voice and data networks.

Several competing protocols are used to protect data transmitted over the public Internet, including Point-to-Point Tunneling Protocol (PPTP). In a process called *tunneling*, packets of data are encrypted and wrapped inside IP packets. By adding this wrapper around a network message to hide its content, business firms create a private connection that travels through the public Internet.

The Web

The web is the most popular Internet service. It's a system with universally accepted standards for storing, retrieving, formatting, and displaying information by using a client/server architecture. Web pages are formatted using hypertext, embedded links that connect documents to one another and that also link pages to other objects, such as sound, video, or animation files. When you click a graphic and a video clip plays, you have clicked a hyperlink. A typical **website** is a collection of web pages linked to a home page.

Hypertext

Web pages are based on a standard Hypertext Markup Language (HTML), which formats documents and incorporates dynamic links to other documents and other objects stored in the same or remote computers (see Chapter 5). Web pages are