Online Monitoring: A Threat to Employee Privacy in the Wired Workplace

As the Internet has become an integral tool of businesses, I believe that company policies on Internet usage have become as common as policies regarding vacation days or sexual harassment. A 2005 study by the American Management Association and ePolicy Institute found that 76% of companies monitor employees’ use of the Web, and the number of companies that block employees’ access to certain Web sites has increased 27% since 2001 (Forbes.com/hwealhtpps2/webseries). Unlike other company rules, however, Internet usage policies often include language authorizing companies to secretly monitor their employees, a practice that raises questions about rights in the workplace. If only companies would stop watching us like flies on the wall. Although companies often have legitimate concerns that lead them to monitor employees’ Internet usage—from a lot of expensive security breaches to reduced productivity—the benefits of electronic surveillance are outweighed by its costs to employees’ privacy and autonomy.

Some experts have argued that a range of legitimate concerns justifies employer monitoring of employee Internet usage. As PC World columnist Daniel Tynan points out, companies that don’t monitor network traffic can be penalized for their ignorance. “Employees could accidentally (or deliberately) spill confidential information . . . or allow worms to spread throughout a corporate network.” (Daniel Tynan, 78) The ePolicy Institute, an organization that advises companies about reducing risks from technology, reported that breaches in computer security cost institutions $100 million in 1999 alone (Flynn). Companies also are held legally accountable for many of the transactions conducted on their networks and with their technology.