Electronic mail (e-mail) has become increasingly important in the workplace. The growth of this new medium of communication has generated important legal questions about the privacy and monitoring of e-mail messages, so much so that most experts strongly recommend that organizations adopt explicit policies about e-mail for their own legal protection. The legal questions concerning e-mail in the workplace include both: (a) employee rights to privacy regarding e-mail messages; and (b) employee obligations to monitor e-mail to ensure a suitable workplace or to prevent illegal behavior. We discuss both of these topics in this chapter, attempting not only to outline current legal thinking in the area, but also to raise questions that managers and policy makers should consider.

It is worth noting at the start that many of the legal issues surrounding the use of e-mail are direct extensions of principles that apply to other forms of communications. Indeed, much of the law that governs e-mail is not legislation that was written explicitly to cover this particular form of communication. Issues of the privacy of employee e-mail messages, for example, are directly analogous to issues of the privacy of employee phone calls or written correspondence. To be sure, there are questions about exactly how legal principles that were established for older communication technolo-
gies should be applied to a new one, and perhaps not all of these questions are fully settled at this point in time, but our understanding of this topic is broadened if we appreciate the application of legal principles across communication media.

PRIVACY ISSUES AND BELIEFS

Many employees probably believe that their e-mail messages should be private. Most employees probably also have thought for a long time that it would be highly inappropriate for supervisors to listen to their phone conversations at work—except perhaps for the monitoring of employees who primarily handle public phone calls, such as tax department workers responding to taxpayer questions. Similarly, most employees undoubtedly would be upset if their employer opened and read their personal correspondence. By extension, employees may also feel that e-mail falls into the same category and that supervisors should not be reading their e-mail without permission, except in certain narrowly defined cases. Many employees undoubtedly use their work e-mail system to send personal messages, both internally and externally, or they may mix personal and professional items in the same message, in much the same way that both may be mixed together in a phone conversation with a colleague. Employees may believe that they are entitled to privacy in these matters, and the fact that passwords are required to access their computer accounts, and thus their e-mail, may be considered confirmation of this belief (Dixon, 1997; Greengard, 1996).

Regardless of what many employees might believe should be the case, their legal right to privacy is quite limited when it comes to e-mail messages. The possible basis for a right to privacy of e-mail messages from the scrutiny of the employer might come from several sources. First of all, the Fourth Amendment prohibits the government from unreasonable searches and seizures, and this restricts public (but not private) sector employers. Second, federal legislation, most notably the Federal Electronic Communications Privacy Act of 1986, provides some protection for communications. Third, many states may have their own constitutional and statutory provisions, which may even go beyond what the U.S. Constitution or federal laws stipulate. Finally, under common law an individual may assert a tort claim for invasion
Related Content

Reputation, Reputation System and Reputation Distribution - An Exploratory Study in Online Consumer-to-Consumer Auctions
www.igi-global.com/chapter/reputation-reputation-system-reputation-distribution/7395?camid=4v1a

Formal Verification of Secrecy, Coercion Resistance and Verifiability Properties for a Remote Electronic Voting Protocol
www.igi-global.com/article/formal-verification-of-secrecy-coercion-resistance-and-verifiability-properties-for-a-remote-electronic-voting-protocol/87425?camid=4v1a
A Secure Hybrid Network Solution to Enhance the Resilience of the UK Government National Critical Infrastructure TETRA Deployment
www.igi-global.com/article/secure-hybrid-network-solution-enhance/53012?camid=4v1a

An Autocorrelation Methodology for the Assessment of Security Assurance
www.igi-global.com/chapter/autocorrelation-methodology-assessment-security-assurance/7411?camid=4v1a