DELIVERING STRATEGIC SOLUTIONS ACCA'S 2000 ANNUAL MEETING

The Internet Age Redefines the Workplace

ACCA Annual Meeting 2000

Delivering Strategic Solutions

October 2-4, 2000

Presented by

Michael F. LaBianca, Esq.

Worldwide Legal Human Resources Manager

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 (408) 526-4000

Garry G. Mathiason, Esq.

Chair, High Technology Practice Group

P ALIGN="CENTER"> Littler Mendelson, 650 California St., 20th Floor, San Francisco CA 94108 (415) 433-1940

DIGITAL WORKPLACE 2000: A Comprehensive Guide To E-Employment Law*

P>

INTRODUCTION

As the calendar rolled over from 1999 to 2000, another change occurred in the United States–a change less apparent but every bit as significant. Sometime near the end of 1999, a national measurement scale tilted from one side to the other: For the first time, the number of persons in the United States who used the Internet outnumbered those who did not. <http://cnn.com/1999/TECH/computing/12/23/more.surfers.idg/ index.html> A February 2000 Gallup Poll confirmed the trend: more than half the respondents had recently used the Internet, up from forty-seven percent in the same category in November 1998. <http://cnn.com/2000/TECH /computing/02/23/Internet.poll/index.html> (And of those questioned, seventy-two percent said that the Internet had bettered their lives!) These surveys confirmed what many already believed–the Internet

continues to extend its impact on the lives of more and more Americans.

The survey results come as no surprise to America's employers. The digital workplace is here. The Internet, Intranets, e-mail, voicemail, facsimile machines, notebook computers and video-conferences are now common features of the American workplace, connecting offices and factories with other workplaces and the entirety of civilization through digital pathways where information and thought travel at the speed of light. It has been estimated that now almost every white-collar job in America requires some level of familiarity with computers and that seventy-five percent of industrial workers are required to have at least elementary computer skills. The effects of the digital workplace are being felt throughout the country. One study suggests that in the past seven years, business-to-business mail has declined thirty-five percent, largely due to the increased use of e-mail. Currently, an estimated forty million employees regularly communicate via e-mail, generating some sixty billion electronic messages each year. John Sheridan, *You've Got More E-mail*, Industry Week, Jan. 24, 2000, at 10. Still other studies estimate that between 250 million and 300 million individuals now use the Internet.

Development of the information superhighway and the digital workplace has not come without problems. The employment law challenges and opportunities of the Internet have confirmed both the grand expectations and dire predictions first published by Littler Mendelson in our 1994 study of the digital workplace. The same technology that serves to increase a company's productivity and sales can also create employment-related litigation risks. For instance, while e-mail can be used to transact business and increase efficiency, it has also been used to broadcast discriminatory remarks about other employees. Similarly, the Internet, which opens doors to the vast resources of the information superhighway, has also opened the doors of some companies to sexually explicit material and copyrighted software downloaded from the Internet.

It is only by fully understanding the characteristics of these new technologies that employers will be able to enjoy the benefits of the digital workplace while minimizing their litigation risks. As one commentator noted, "Once a new technology rolls over you, if you're not part of the steam roller, you're part of the road." Lisa Napoli, *The Big Net Story Was Size Itself* (Dec. 30, 1998) <http://www.nytimes.com/library/tech98/12/cyber/articles/>. Today's businesses need to make sure they do not become part of the road by learning as much as possible about digital technology and its infinite capabilities. They need to learn how to take advantage of this technology and how to avoid the dangers created by its use in the workplace.

Employers can take specific and immediate action to accomplish these goals. This chapter is an effort to provide the reader with a road map of the most common legal issues facing employers today regarding the digital workplace and to provide possible solutions. The theme of this chapter is that a digital workplace employer who can recognize employment law issues and ask the proper questions can reduce the likelihood of litigation and legal problems. Throughout this chapter, references are also made to material contained within The 2000 National Employer® that addresses the legal issues discussed in this chapter in more detail. Like many of Littler Mendelson's groundbreaking initial efforts (*e.g.*, Workplace Violence Prevention and the Law of Training), our year-2000 digital workplace chapter is intended to create an analytical structure for a new area of employment and labor law. In subsequent years a more complete listing of issues and practical suggestions will emerge. We welcome your critical review of this analysis in progress. Your ideas and observations coupled with the experiences of our four hundred employment attorneys will shape our subsequent writings on digital technology as it redefines the workplace.

> P ALIGN="JUSTIFY">Ben Arman sat uncomfortably on the witness stand of a federal district court. He works for a major manufacturing company and called in sick during a recent work stoppage. The attorney for the company turned her piercing eyes upon the witness. "Isn't it true you called in sick, not because you were actually sick, but because you wanted to support the Union's grievances?"
> Mr. Arman, appearing very uncomfortable, hesitantly answered, "No." The attorney immediately introduced into evidence the transcript of an America Online chat

group. She turned to Mr. Arman and stated, "Isn't it true that you sent the following message while participating in an Internet chat room? 'Our employer is unfair and deserves to be shut down. Unfortunately our f _ _ _ _ _ _ laws are so twisted that it is necessary to claim illness to get justice.'" The red-faced employee responded, "I thought that was a confidential communication."

Employee Use Of The Internet

Welcome to the age of the Internet as it redefines the workplace. Often referred to as a network of networks, the Internet is a worldwide, global, interconnected network of thousands of public and private computer networks used by millions of people throughout the world. It was originally developed for the government for the purpose of securely linking computers around the country so that top-secret information and research could be safely and confidentially shared among the Defense Department, scientists, and academics. Gordon D. Lee, Esq., *Legal Bytes: Should Attorneys Use the Internet?* 44 Rhode Island Bar J. 27 (Dec. 1995). While the Internet may have been created as a government tool, as the surveys previously cited demonstrate it is now used by most Americans, from children to senior citizens, and it is used everywhere, including homes, schools, and workplaces. No one is responsible for managing the Internet, and it operates with few, if any, controls. Enormous data transfers take place on the Internet each day. The Internet allows people to connect with others around the world and to exchange ideas and information economically.

In the workplace, the power of the Internet has been discovered and its use has increased exponentially over just the past five years. The Internet allows people to connect with others around the world to exchange ideas and information for very little cost. Additionally, employees can access myriad nonjob-related sites through the Internet, including news and entertainment sites, as well as pornographic and other inappropriate sites. Employees can buy goods online, and might even use a company credit card to do so. Indeed, the International Data Corporation, a market research company, has predicted that the number of "customers" who can be reached for business collaboration and sales over the Internet will grow from 68.7 million in 1997 to 319.8 million in 2002, with a compound annual growth rate of thirty-six percent.

Business Use Of The Internet

The Internet has revolutionized the way that companies do business. Today, all major companies have their own Web sites and do much of their advertising on the Internet. An overwhelming number of companies has begun to sell products over the Internet, and now virtually anything can be purchased online. E-commerce is booming. Dell Computer Corporation, one of the first major companies to move into e-commerce, now has online sales of fourteen million dollars per week. Bill Gates, *Bill Gates' New Rules*, TIME, Mar. 22, 1999, at 72, 82. Some companies, such as Egghead Software, have moved their entire operations online–selling products only over the Internet. If a task needs to be done, workers are increasingly turning to the Internet to do it. Between nineteen million and twenty-six million Americans have access to the Internet at work. Each worker spends approximately six hours per week online. David Plotnikoff, *Work, the Web & the Watchers* (Oct. 10, 1998) <http://www.mercurycenter.com/premium/
front/docs/workweb10.htm>. Employees go online and visit "OfficeDepot.com" when they need to order supplies. They get on the Internet to track a package that is late in arriving. Employees now perform all types of work-related research over the Internet instead of going to a library or hiring an outside research firm. When employees need information, from directions to a client's office to statistics on trade in China, they are increasingly turning to the Internet for answers. Employees can now even use the Internet to enroll in a healthcare plan or access their 401(k) information.

Virtually every activity in today's workplace can involve the Internet. Résumés are accepted and interviews are conducted online. In addition to using the Internet to find qualified employees, companies are using it to conduct performance evaluations. The Internet is now being used to deliver efficient and effective training without requiring the employees ever to leave their desks. It can also be a powerful tool in the hands of a

union. Potential union members can use the Internet to contact a union about joining and to transmit information about pay and working conditions to the union. The Internet is even starting to play a role in disputes between employers and employees. Recently, the world's first labor strike over the Internet took place. The workers staged an online strike that rendered many of the company's Web pages unreadable. David J. Loundy and Blake A. Bell, *E-Law Update #6 Part 2* (Oct. 21, 1998) <http://www.infowar.com/law/law_103098c_j.shtml>. In addition, the Internet is now being used to settle disputes. Instead of heading off to court to settle disagreements, some people are making online visits to virtual arbitrators. As of now, online arbitrators only decide disputes that deal somehow with the Internet or the online world. However, it is likely that in the future online arbitrators will deal with all types of disputes.

Employee Communication Via The Internet

The Internet has also changed the way employees communicate with one another. Americans send 2.2 billion e-mail messages per day. When compared with the 293 million first class mail messages sent each day, it becomes clear that e-mail is taking over. David L. Marcus, *E-mail Nation*, U.S. News &World Rpt., Mar. 22, 1999, at 54. E-mail has sped up the workplace. While days go by before mail is received through the post office, e-mail is received just seconds after it is sent. E-mail has changed communication in another way–it has changed the people with whom we choose to communicate. A first-year associate in a large company who would never consider walking into the company president's office or telephoning her to ask a question might very well send an e-mail to the president to inquire. Thus, e-mail has expanded the realm of people with whom employees will communicate, flattening the hierarchical structure of many businesses. Bill Gates, *Bill Gates' New Rules*, Time, Mar. 22, 1999, at 72, 74.

By allowing employees to remain connected to one another regardless of location, the Internet has made the traditional office much less important. Some companies have given up their brick-and-mortar offices entirely. For example, Verifone, a company that makes credit-card readers, has no corporate office. The three top executives live in three different cities and communicate over the Internet. There are now virtual hard drives that store data and are accessed from the World Wide Web. A product called Virtual Workplace creates a boardroom in cyberspace where teams can share workspace on the Web and can collaborate in real-time. Online.briefcase is a service that connects an employee's phone directory and calendar to the Web. Netcams (Internet videophones) that can be connected to almost any personal computer allow employees to hold meetings over the Internet. It seems as if anything that needs to get done can get done on the Internet.

CYBERSABOTAGE

The Internet is a useful and oftentimes invaluable tool in the workplace. No force will reverse the trend to build the Internet into our workplace lives; however, organizations need to be aware of the dark side of the Internet. It is here that our inquiry into employment and labor law begins. Hackers and cybercriminals are constantly looking for valuable company information and present a real threat to any company with Internet access. According to a Computer Security Institute report, approximately two-thirds of the five hundred twenty companies, government offices, and universities surveyed had experienced computer break-ins or other security breaches in the past twelve months. David Plotnikoff, *Identifying Net Criminals Difficult* (visited Mar. 8, 1999) <http://www.infowar.com/class_1/class1_032698A_j.html-ssi>. While it is important for employers to be aware of the security risks posed by computer hackers and cybercriminals, they must also be aware of the dangers posed by their very own employees.

The Internet presents a vast number of ways for employees to harm one another and their employers. From cyberstalking to unleashing a destructive computer virus into the company network, the Internet is creating endless opportunities for angry or troubled employees to commit cybersabotage. The anonymity of cyberspace gives employees the courage to do and say things they would not do or say in person and actually encourages crime because it is so much harder to get caught when one is anonymous. The Internet is also appealing to many angry employees because severe damage can be caused with very little effort.

Espionage & Sabotage

How secure is the digital workplace against access or vandalism by disgruntled employees or outside competitors? Can employees access confidential personnel or medical information from a desktop PC? Does the company have a policy forbidding the transmission of sexually vulgar or offensive communications? What procedures exist to prevent and reduce damage resulting from accidental or malicious security lapses?

The FBI reported that it opened . . . "computer-intrusion cases" in 1998, and . . . such cases last year–more than double the previous year. <http://www.infowar.com/law/00/law_026100a_j.shtml> This probably represents a minuscule portion of the actual magnitude of the threat. Corporate file theft and intrusion online is a ten-billion-dollar business. Opening company computer networks for remote access and Internet connections increases a company's risk in protecting trade secrets, and can make a company vulnerable to computer-virus attacks. Furthermore, employers risk theft and fraud from employees making online purchases with company credit cards.

In a survey by Security Dynamics Technologies, Inc., ninety-one percent of the information security managers surveyed reported that corporations face an increased risk to the security of their corporate data contained on computer networks. Over half of those surveyed were aware of at least one unauthorized access to their networks. One in ten reported significant financial losses (including a number of losses in excess of one hundred thousand dollars) from network break-ins. The most significant reported security threat is from disgruntled ex-employees followed by e-mail break-ins, unauthorized access to computer networks (such as unauthorized access from the Internet), and unauthorized dial-up access. Eighty-two percent of those surveyed cited e-mail breaches as a potential security risk. An example of such a breach occurred at the Lillehammer Olympics. David Strom, in an *Infoworld* article on May 16, 1994, reported that reporters at the Olympics managed to access and read Tanya Harding's e-mail messages on the Lillehammer Olympics computing system by hacking her password.

The simple truth is that no digital workplace is inherently immune from espionage and sabotage. For example, one office equipment distributor had its voicemail system accessed by a rival distributor who stole customer inquiries. The rival then contacted the customers and offered attractive terms on its equipment. E-mail systems are easily accessed. The business press is filled with examples of competitors gaining access to e-mail systems and using the information to their advantage.

Beyond espionage concerns, employers must also consider the possibility that an employee may gain access to highly confidential information stored on the system and may sabotage the system by destroying files or directories or otherwise using the system in an unlawful manner. Such information as financial records, medical records, digital data exchanged between companies, personnel records, receipts and shipping information, payroll data, telephone records, and word processing data is all being stored on computer networks. Consider the potential ramifications of an employee's gaining access to confidential medical information and then informing company personnel, via the e-mail system, that a fellow employee has HIV.

These examples clearly illustrate the vulnerability of the digital workplace. Employers must endeavor to keep their digital workplaces private and confidential or risk liability for their failure to address the problem. If an employer has not sought to protect its system from unauthorized access, an employer may be considered negligent for this failure. This is especially true because that technology exists that can accomplish this task. Employers can increase security by hiring an affordable computer network security consultant. Such consultants should not be hired only after a security problem arises. Security consultants can be of the most benefit if they are hired to prevent security problems from happening in the first place.

Encryption

E-mail, digital files, and digital networks are not always secure enough to guarantee the confidentiality of the

information contained in the system. Employees using e-mail to communicate with clients and colleagues must be sure that materials sent electronically are secure. Sending e-mail messages and/or files *appears* safe, as the sender can make sure to send the file or message directly to just one person, with no stops along the way to intercept or change the message. The appearance of safety however, is deceptive: e-mail can be read at any number of points in cyberspace. E-mail can be read by any number of people, including staff at online service providers and hackers sampling e-mail on the Internet. Consequently some e-mail users are turning to encryption, a form of encoding, to protect sensitive materials.

Encryption is a method of scrambling digital data to thwart unauthorized access by turning a message into gibberish, readable only by the person intended to read the message–someone who has the proper key. The most powerful forms of encryption have two keys: one public, the other private. The two-key system works like this: If supervisor Ann wanted to send manager Bill a message and be certain that only Bill could read that message, Bill could give Ann the "public key" (a code). She would encrypt her message with his public key and an encryption program. Then Bill could decrypt it, using his private key. The most popular encryption program, Pretty Good Privacy (PGP) is claimed to be virtually impossible to crack.

Unfortunately, the encryption technology may also be used by employees to block access by the employer. This may severely hamper an employer's ability to enforce its policies and procedures. For example, an e-mail system may be encrypted in such a way that the sender of the message can become virtually invisible. If this is allowed to happen, the employer's ability to regulate and monitor the communications between employees and supervisors could be severely hampered. An employer would never know where an offensive message came from or from whom it came. In a similar way, if two employees are able to communicate in absolute encrypted privacy and secrecy, there is no way to monitor the communications effectively.

Because companies need to take all measures to protect confidential information, encryption technology is becoming an absolute necessity. Any employer who uses encryption technology must be aware, however, this technology is classified as a munition. Thus, there are many laws governing the use of such technology in dealings with other countries. If an employer who has dealings with businesses or people outside the United States wants to use encryption technology, an attorney should be contacted in order to ensure that all laws dealing with encryption technology are followed.

Another way to prevent unwanted disclosure of sensitive information is to adopt an employment policy that forbids unauthorized access to and/or transmission of certain confidential information. A carefully drafted employment policy that addresses these issues is an absolute necessity in the digital workplace. The sample policy regarding voicemail and e-mail found at the end of the chapter contains language that may be helpful in this regard.

HARASSMENT

The digital workplace will likely become a breeding ground for sexual harassment claims. Sexually offensive e-mail and voicemail messages will increasingly be used by plaintiffs as evidence of a hostile work environment. A manager of information systems and business processes at Eastman Kodak Company has stated that harassment complaints are the most prevalently reported e-mail abuse in his company. The case law is beginning to reflect such abuses. In a federal case, a human resources manager brought a sexual harassment and sex discrimination claim against her employer for terminating her for failing to report that she had been sent several e-mail messages that contained a numerical code that incorporated a list of approximately seventy-five profane words and phases. *Miller v. U.S.F. & G.*, 1994 U.S. Dist. LEXIS 10541 (D. Md. May 13, 1994). In *Strauss v. Microsoft Corp.*, 814 F. Supp. 1186 (S.D.N.Y. 1993), a female employee sued Microsoft for gender discrimination relying partly on evidence that her superior sent an e-mail message to the entire staff that "contained sexual innuendo referring to male genitalia." *Id.* at 1189 n.3. Sexual harassment claimants are increasingly using e-mail messages and voicemail messages to support their charges.

In addition, the Internet is increasingly being used by employees to harass other employees. Some employees download obscene material onto employer systems or allow pornographic materials to appear on their PCs. The open viewing of sexually explicit Web sites can fall within the definition of intimidation that can create a "hostile working environment." One survey released in April 1997 showed that employees at I.B.M., Apple Computer, AT&T, NASA, and Hewlett-Packard call up the online edition of Penthouse Magazine thousands of times a month. In an article entitled "*PC Profanity: Sexual Harassment*," a University of Illinois speech professor was reported to have received an e-mail message that contained the image of a pair of breasts constructed out of punctuation marks. In the same article, a writer was reported to have received rape threats over her e-mail. These examples demonstrate that the use of e-mail or voicemail in a sexually offensive manner is limited solely by the imagination of one's workforce. One employer reportedly faced six claims of harassment due to an employee's downloading of an adult bulletin board onto the company's computer system.

Many employers have tracking systems that allow them to monitor employee use of the Internet. These tracking systems provide employers with a list of each Web site visited by each employee who accesses the Internet. This type of system may be useful in assisting employers to discover improper use of the Internet. However, a tracking or monitoring system may also prove to be a liability–an employee may use the tracking information as evidence that employees regularly visit sexually explicit Web sites. This evidence could be used to support a claim that the employer maintained a sexually permissive work environment.

Given that virtual teams mainly communicate with each other over the computer network, employers must remember that a record is created of all these communications. This record remains long after an offensive e-mail is deleted and can be used against the employer in harassment and discrimination cases. Cyberspace reduces inhibitions and often causes people to say things online that they would never say in person. Nuance is not easily communicated online, and a virtual team member may offend another member without even trying. A virtual team can be made up of members from countries around the world. However, the cultural differences among virtual team members living in different countries can create problems. What may be a perfectly acceptable online communication between two workers in the United States may be very offensive when sent to a female worker in Saudi Arabia. Employers would be well served by facilitating training of virtual workers on how to interact effectively with coworkers from different countries.

Harassment that occurs in the virtual world of cyberspace is harder to stop than harassment in the real world. It is often more difficult to determine the identity of an Internet harasser. In most sexual harassment cases, the harasser's identity is clear. However, given the anonymity available to users of the Internet, the identity of Internet harassers is often unknown. The ease with which one can assume another employee's e-identity was demonstrated in a recent case in Washington state, *Hatch v. Fred Meyer, Inc.*, 1999 Wash. App. LEXIS 385 (Mar. 1, 1999). There, a female retail clerk sued her employer, alleging that she had been subjected to a sexually hostile work environment. The sexual harassment was alleged to have occurred when a store manager, noticing that the plaintiff had failed to sign off from her computer terminal properly, sat down at her terminal and sent an e-mail to the plaintiff's supervisor. The e-mail purportedly sent by the plaintiff stated that, "I have been watching you from afar and I really think we need to get together. I want to meet you in a dark place and rip your pants off and have my way with you . . . meet me tonight . . . missing you." *Id.* at *9-10. Because the supervisor who received the e-mail realized that it was likely a vicious prank committed by one of the plaintiff's coworkers and took appropriate action, the sexual harassment suit was dismissed.

Harassers have many ways to keep from being discovered. Anonymous remailers are frequently used to ensure the anonymity of online harassers. A person wishing to be anonymous simply has to send his or her message to an anonymous remailer such as the one available at <www.anonymizer.com>. The remailer substitutes a fake header and then sends the message. Thus, anyone reading the message will see inaccurate information about the sender's identity.

Harassment over the Internet raises some interesting questions that have not yet been answered. For example,

how far does an employer have to go to stop Internet harassment? Is it enough simply to change the victim's e-mail address? What if the harasser is using an anonymous remailer like the one described above? Is the employer required to file a lawsuit and subpoena "anonymizer.com" records in order to determine the true identity of the harasser? These questions undoubtedly will be answered once such cases are brought to court. Until then, employers need to be aware of the risk of Internet harassment. Employers must take such harassment seriously and work to prevent and correct it with the same vigilance accorded other forms of harassment.

Accordingly, an employer's e-mail and voicemail policy should have a statement prohibiting messages containing offensive or sexual materials and should place an obligation on an employee to report such messages if received. The policy should state that e-mail and voicemail are to be used for business and professional reasons, not personal reasons. Such a statement may not actually prevent an employee from using e-mail and/or voicemail in a sexually hostile manner. However, the policy will be useful for discipline purposes and to defend against a claim of sexual harassment. Employers should emphasize in their policy that employees should not refer to or denigrate a person's race, color, religion, sex, age, national origin, disabilities, or physique. For a sample statement, see the e-mail and voicemail sample policies at the end of the chapter. (For a more extensive discussion of sexual harassment, see Chapter 7 of The 2000 National Employer®.)

Cyberstalking

Stalking can be considered a form of workplace harassment and violence. The Internet has created a new form of stalking known as cyberstalking. As employers can be held responsible under a variety of different liability theories for acts of workplace violence, they need to be aware of the potential for workplace violence that the Internet presents. (For a more extensive discussion about an employer's duties with regard to preventing and correcting workplace violence see Chapter 34 of The 2000 National Employer®.)

A cyberstalker pursues, harasses, and threatens his or her victim through e-mail messages, postings on Internet message boards and discussion in Internet chat rooms. In *Internet America Inc. v. Massey*, Case No. 96-10955C (Tex. D. Ct., Dallas Cty., Oct. 14, 1996), a court ordered a cyberstalker to stop sending harassing, threatening, and offensive messages over the Internet. The court order was posted on the Internet and later delivered to the cyberstalker in person. In this case, the cyberstalker was threatening and harassing the owners of an Internet service provider called Internet America by posting harassing, embarrassing, and threatening messages about them in Internet chat rooms. One message said "I have a gun and I know where you are."

A recent cyberstalking case was particularly disturbing. In this case, the cyberstalker is accused of attempting to set up a rape of his victim by posing as the victim over the Internet. He is said to have forged e-mails and postings on "personals" Web sites, claiming to be the victim and stating that she had fantasies of being raped. Six men actually came to the victim's home in response to the forged postings and e-mails. The case against the cyberstalker, *People v. Dellapenta*, Case No. BA 177445 (L.A. Sup. Ct. 1999), is the first prosecution under California's newly updated antistalking law. The law was recently updated to include threats by e-mail, pagers, and other forms of electronic communication. Cal. Code Civ. Proc. § 527.8(b)(3) (e-mail correspondence included as one form of a course of conduct which may constitute stalking and justify a TRO or injunction for civil harassment).

Cyberstalking can easily turn into real-life stalking. As Internet access at the workplace increases, so too does the risk of workplace violence. Employers must be aware of the dangers associated with stalking over the Internet and must take the issue seriously.

Cyberdefamation

The digital workplace raises a number of issues related to the tort of defamation. In general, defamation encompasses any false and unprivileged communication, either oral or written, that has a tendency to injure a person in his or her occupation or reputation. This would include intracorporate discussions or exchanges of information that are not essential to a termination or other employment decision. *Frankson v. Design Space Int'l*, 380 N.W.2d 560 (Minn. Ct. App.), *aff'd in part and rev'd in part*, 394 N.W.2d 140 (Minn. 1986). Libel, a type of defamation, is a tort consisting of a false and malicious publication printed for the purpose of defaming someone. (For a more extensive discussion of defamation, see Chapter 12 of The 2000 National Employer®.)

Sources Of Electronic Libel

Potential liability for defamation in the digital workplace can arise from a number of sources. For example, e-mail, voicemail, and integrated computer networks have been designed to facilitate and encourage the rapid exchange and storage of information. Consider the situation where someone has gained unauthorized access to information stored or transmitted on an e-mail, voicemail, or computer system or where an employee accesses the personnel department's e-mail, voicemail, or computer network. In less than a second, the employee will likely acquire a great deal of potentially defamatory information, including performance evaluations and medical information, which has been stored or is being transmitted on these systems. Moreover, the information can be transmitted in seconds to other employees' machines or terminals. Has the information been published to the unauthorized employee for defamation purposes? Could the employer be held liable for defamation as a result of the unauthorized entry?

Posting libelous statements over the Internet has come to be known as "cyberlibel" or "cybersmearing." As Internet usage is increasing, so too is this kind of cybersabotage. Disgruntled employees with Internet access are increasingly venting their anger by making false and harmful statements about their employers and broadcasting these statements throughout cyberspace. The Internet has given angry employees a much larger forum in which to air their grievances. No longer does an angry employee have to settle for simply scrawling an insult about a supervisor on the breakroom wall. He or she now can head straight for the Internet, ensuring that thousands of people will hear comments about the employer. And companies are increasingly fighting back and suing the anonymous posters of libelous statements.

Recently, libelous messages about a maker of medical equipment were posted on the Internet. The messages described the company's future as "uncertain and unstable" and were anonymously posted on a Yahoo! investment message board. The company subpoenaed Yahoo! for information about the anonymous user and discovered that the messages were posted by a former chief operating officer. The accused former officer claims that someone misappropriated his online identity and that he did not post the messages. Jennifer Sullivan, *Sticks and Stones on the Net* (Nov. 5, 1998) <http://www.wired.com/news/news/business/story/16059.html>

Rumors posted on the Internet are especially damaging because they are so easily spread. Once the rumor is posted in cyberspace, it takes on a life of its own. One person who reads the rumor can forward it with ease to hundreds of friends and can post it to an Internet bulletin board where it will be read by thousands of other people, each of whom can forward the rumor to all of his or her friends. These Internet rumors are impossible to control and can circulate on the Internet for years–long after the anger of the disgruntled employee who posted the rumor has subsided. The rumors are often disguised as urgent warnings to consumers and contain a request for the reader to forward the message to everyone he or she knows. While the stories behind the rumors are not real, the damage suffered by the companies who are victims of the rumors is very real. There are several Web sites that list false Internet rumors and debunk each of them. One such site is <http://urbanlegends.miningco.com>. However, by the time such rumors are dispelled, irreparable damage to a company's reputation often has already been done.

- Blue Mountain Arts, a small, family-owned business that offers free digital greetings cards was

recently devastated by a false Internet rumor. Someone posted a rumor on the Internet that Blue Mountain greeting cards contained a virus that would destroy the recipient's computer system when the card was opened.

- Tommy Hilfiger, a clothing designer, was also the victim of a false Internet rumor. The rumor stated that the designer said on the Oprah Winfrey Show that he wished minorities would not buy his clothing. The Internet message asked everyone who read it to boycott Tommy Hilfiger clothing.

- False Internet rumors about Taco Bell being infested with roaches and about Kentucky Fried Chicken deep-frying rodents have been circulating on the Internet for years. While it is not known if disgruntled employees were behind any of these rumors, they likely could have been.

The Internet is a powerful tool, and when used by an angry employee, it can destroy a company's reputation.

An angry employee can also do serious harm to an employer by posting offensive messages or advertisements and attributing the posting to the employer. A recent case, *Zeran v. America Online, Inc*., 129 F.3d 327 (4th Cir. 1997), illustrates how much trouble can be caused by these false postings. While the case did not involve a disgruntled employee, a situation like the one described in the case could easily occur between an employee and employer. Mr. Zeran was the victim of a cruel hoax in which an anonymous person attached Zeran's name and home phone number to several postings on America Online's bulletin boards. The postings were advertisements for t-shirts and other products with incredibly offensive slogans that glorified the bombing of the Alfred P. Murrah Federal Building in Oklahoma City. Soon after the ads were posted, Zeran began to receive angry phone calls, including death threats. At one point, Zeran was getting an abusive call every two minutes. An Oklahoma City radio station learned of the ads and one of the announcers instructed listeners to call the number to complain. After the radio announcement, the number of death threats increased. Zeran could not change his phone number because he ran his business out of his home and relied on the phone number for his business. Zeran told America Online about the false ads. The company told Zeran that they would remove the ads from the bulletin board, but said that company policy prohibited it from posting a retraction of the false ads. Zeran then sued America Online for not printing a retraction and for taking too long to remove the ads. He lost his case.

If an angry employee were to place offensive ads like the ones in *Zeran* and attach his or employer's name to the ads, the damage to the company would be staggering. Employers need to be aware of the risk of this kind of cybersabotage so that they can react quickly and minimize damage if it happens to them.

Defamation claims brought by terminated employees have been common in the employment arena. What is new, however, is that the damages awarded in defamation cases have dramatically increased. For example, a jury in North Dakota awarded $1.2 million in general damages and $700,000 in punitive damages to a man the jury found had been defamed when his former employer sent a series of letters falsely stating that he had been terminated for good cause. *Vanover v. Kansas City Life Ins. Co.*, 535 N.W.2d 424 (N.D. 1995). Awards of over $2 million, $150,000, and $100,000 are no longer uncommon.

Written communications are fertile ground for litigation. Any intracompany communication may constitute publication, even though the publication may be privileged. For example, although employers usually enjoy the privilege of communicating disciplinary and performance information, employees have sued for disparaging remarks made about them in disciplinary notices and written evaluations. Similarly, memoranda prepared during internal investigations of misconduct such as alleged sexual harassment have also generated litigation. Although employers engaged in an investigation of an allegation of sexual harassment will generally be protected by the EEOC's requirement that employers take all steps necessary to prevent harassment, this is not a guaranteed form of protection. Furthermore, while idle comments made by two employees who are complaining about a third party are not necessarily defamatory, such a comment sent via e-mail may be

defamatory because company property was used, and the record is permanent.

Preventive Measures

Liability in this area may be reduced using a variety of techniques. An employer can begin with an e-mail and voicemail policy that carefully sets out the types of messages that may be transmitted over the system. This policy would forbid any offensive or disrupting messages. An employer may also want to implement a monitoring system to check periodically the content of its employees' e-mail and/or voicemail messages. A recent survey found that twenty-seven percent of companies already monitor internal e-mail to check for inappropriate material. Jeffrey L. Seglin, *You've Got Mail. You're Being Watched*, N.Y. Times, July 18, 1999, § 3, at 4. Such a monitoring system must be carefully designed and would have to include advance notice to employees.

Another option would include the use of encryption technology. Encryption technology exists to protect stored, confidential information from access by unauthorized employees. This technology can be a major barrier to the release of potentially defamatory information. An employer may also include confidentiality provisions in an e-mail or voicemail policy to protect the confidentiality of such transmission. A simple statement that–stating all such messages are considered confidential and should be read only by the addressee, by those authorized by the addressee, or by the employer in its normal monitoring–will go a long way toward reducing the release of potentially defamatory information. (The sample e-mail and voicemail policies included at the end of this chapter include suggested language in this regard.)

Damaging Web Sites

Disgruntled employees can also vent their anger by logging onto a Web site called "www.disgruntled.com." Here disgruntled employees can post their stories about employers and can read thousands of similar stories from other dissatisfied employees. When an angry employee visits the Web site, he or she is promptly instructed: "Tell us your stories about why your job sucks, how miserable your boss is and what you do to vent your frustrations or get even."

While the majority of postings do not mention the employer by name, the site can still cause problems for employers. For example, one section is entitled, "Getting Even: Tales of Revenge and Sabotage." This section is particularly problematic because it supplies innovative and innumerable ways to sabotage one's employer. For example, an employee at a restaurant explained in his posting exactly how to go about destroying a restaurant business. He explained how putting into the drains fat trimmed from meat destroys the plumbing system, and how placing powerful magnets near the computers destroys the computer system. He also extolled the virtues of introducing roach eggs and mice into the manager's office.

In addition to logging onto "disgruntled.com," employees can create their own Web sites to express their anger. These Web sites can be very damaging to a business. Employees use these sites to complain about their alleged mistreatment, to invite others who have experienced similar treatment to post their stories, and to urge people to think twice before purchasing the employer's products, using the employer's services, eating at the employer's restaurant, etc. In addition to complaining about companies on these Web sites, creators of these sites also often use them to start untrue rumors about companies. For example, a site created to complain about a major airline was the source of a nasty and completely false rumor about a passenger who died from a heart attack because it took the crew more than thirty minutes to realize that he was unconscious. Jerome & Taylor, *Liar, Liar. (Unscrupulous Web Pages)* (Dec. 11, 1998) <http://www.infowar.com/class1/class1_121198A_j.shtml>. How many people heard this rumor and chose a different airline?

Employers should be aware of what is being said about them on the Internet. Employers can hire one of several services that actually search through the thousands of chat rooms and discussion groups that are on the Internet to see what is being said about specific companies. If an untrue rumor or defamatory statement is

found, the company can then post a corrective message and take any necessary legal action against the person who posted the message.

Trademark Infringement

Many of the sites mentioned above have addresses that contain the company's name. Companies are fighting back and suing the creators of these sites for trademark infringement. U-Haul brought a trademark infringement and libel suit against two consumers who launched the "U-Hell Web site." The case was dismissed for lack of jurisdiction, but U-Haul plans to refile the case in another state. David Segal and Caroline E. Mayer, *Angry Consumers Vent on the Net*, S.F. Chron., Apr. 5, 1999, at E2. In addition, Bally Total Fitness sued the creator of the Web site, "ballysucks.com" for trademark infringement. However, the judge refused to order a shutdown of the site. David J. Loundy and Blake A. Bell, *E-Law Update #8, Part 1* (Dec. 28, 1998) <http://www.infowar.com/law/law_122898h_j.shtml>. While these sites were created by angry consumers, they could just as easily have been created by disgruntled employees.

Trademark infringement claims against complaint Web sites are not likely to be successful. In order to prove trademark infringement, a company must show that the offending mark is "likely to cause confusion or to cause mistake or to deceive." The Lanham Act, 15 U.S.C. § 1114(1)(a), (b). As sites such as the "U-Hell Web site" are clearly unofficial and are not likely to confuse consumers, trademark infringement suits will probably fail. However, if false and damaging statements are made on the sites, companies may prevail in libel lawsuits.

Cyberblackmail

Angry employees can also use complaint Web sites to force employers to settle cases. Imagine this scenario: An employee is involved in a harassment suit against his employer. The employer is willing to settle the case for one hundred thousand dollars but the employee wants two hundred thousand dollars. In an effort to convince the employer to pay the two hundred thousand dollars, the employee creates a complaint site that contains the company's name in the address, lists horror stories about the company, and encourages people to stop using the company's products. The company will likely be persuaded to settle the case for two hundred thousand dollars after weighing the potential damage caused by the complaint site.

A situation similar to this hypothetical recently occurred between two angry consumers and a van company they were suing. The consumers created a complaint site, the consumers' lawyer advised the company to take a look at the site, and ten minutes later reportedly, the company settled the claim on the condition that the site be shut down. David J. Loundy and Blake A. Bell, *E-Law Update #9, Part 1* (Jan. 18, 1999) <http://infowar.com/law/99/law_011899b_j.shtml>. Evidently, complaint sites can be very powerful bargaining chips.

Personal Information Posting

While employers face danger from employees who post untrue information on the Internet, the posting of accurate information for millions to see can be just as harmful. Recently, an angry consumer posted the Social Security numbers, home addresses, phone numbers, and vehicle-license records of several employees of the collection and credit-reporting agencies that he believed had wronged him. He even posted maps to some of these people's homes. Citing the importance of respecting free speech on the Internet, a federal judge recently upheld the consumer's right to post this information on the Internet. Peter Lewis, *U.S. Judge Upholds 'Offensive Web Site'* (July 18, 1998) <http://archives.seattletimes.com/cgi-bin/texis/web/vortex/display?storyid=48255&query=sheehan> (discussing *Sheehan III v. King County*, No. C97-1360 OWD (W.D. Wash. 1998)). While this case involved an angry consumer rather than an angry employee, the situation could arise just as easily between an employer and an employee.

E-mail Abuse

E-mail offers enormous benefits to employers and employees. It encourages intracompany communication, increases productivity, and reduces the need for inefficient telephone calls, paper memos, and face-to-face meetings. Workers use e-mail for more than just messages: E-mail can be used to send inventory lists, minutes of meetings, drafts of documents, business strategies, or records of important business decisions. However, e-mail also has enormous potential for workplace mischief and can lead to dramatic developments in employment litigation. For example, a recent survey found that eighty-four percent of the nation's workers admitted to sending personal e-mail from the workplace. Keith Naughton *et al.*, *Cyberslacking*, Newsweek, Nov. 29, 1999, at 62.

As the use of e-mail grows, so too does the risk of liability from e-mail statements. Because of e-mail's informal nature and perceived impermanence, people often use e-mail to send messages that may be too candid to "put in writing," or inappropriate. Most e-mail systems create a complete record of the communication. The systems capture the exact text that users send and receive. Additionally, e-mail records usually store information regarding their transmission and receipt, including the names of the sender and recipient, the dates and time that the messages were sent and received, and an acknowledgment that the e-mail was retrieved. This information may be of great value in demonstrating what personnel were involved in making particular policy decisions, and what officials knew, and when they knew it. The lesson is clear: unless back-up files are routinely cleaned out, digital communications remain stored indefinitely on a hard drive or disk, waiting to be found by the ingenious computer consultant hired by the resourceful attorney who was hired by a discharged and disgruntled former employee.

Employers must be aware of the trouble an angry employee can cause by misusing the e-mail system. Recently, a Pentagon official was the victim of e-mail abuse. He received a never-ending barrage of unwanted e-mail messages from companies trying to sell him products over the Internet. He enlisted the help of the Pentagon to uncover the culprit and found that a former employee was behind the annoying e-mail messages. Evidently, the employee had been given a "Highly successful" job rating rather than an "Outstanding" rating in 1995 and was now retaliating years later. David J. Loundy and Blake A. Bell, *E-Law Update #7* (Nov. 18, 1998) <http://www.infowar.com/law/law_120798a_j.shtml>.

In another example of e-mail abuse, a disgruntled former employee sent periodic mass e-mailings to thousands of current employees, warning them about potential layoffs and telling them not to trust management. The company sued to stop the e-mails. A Sacramento Superior Court recently held that the mass e-mails constituted trespass and issued a preliminary injunction that prohibited the employee from sending any additional e-mail messages to current employees at work. *Intel Corp. v. Hamidi*, 15 IER (BNA) 464 (Cal. Sup. Ct. April 28, 1998). Some cases in which misuse of e-mail resulted in litigation include:

- Two African-American employees of a large investment banking firm brought suit demanding twenty-five million dollars each in damages due to a racist e-mail that was circulated among the white employees. While the federal court judge dismissed the suit on the grounds that one racist e-mail could not form the basis for a hostile work environment, the judge did allow the employees the opportunity to amend their complaint. The case was later settled. *Owens v. Morgan Stanley & Co., Inc.*, 1997 U.S. Dist. LEXIS 10351 (S.D.N.Y. 1997) (case later settled).

- A $2.5 million sexual harassment suit alleged that a male supervisor made frequent lewd remarks to a female employee via company e-mail. *Pamper Barber v. Calsonic Int'l, Inc.* (Tenn. 1995) (suit settled out of court for undisclosed amount).

- Chevron Corporation settled a case brought by four female employees who alleged they were sexually harassed through e-mail. The case settled for $2.2 million, plus legal fees and court costs. Chi. Daily L. Bull., Vol. 143, No. 230 (Nov. 24, 1997).

It is sometimes difficult to determine the true sender of a message, particularly if the sender wishes to hide his

or her identity. This is due, in part, to the growth of anonymous "remailers." Remailers are relay stations on the Internet that cloak the identity of every user who sends a message through them. It works as follows: An individual user sends an e-mail to a newsgroup run by the remailer. The remailer then strips the name and return address off the posting and replaces them with a new name and return address. The system also adds a pseudonym, making responding to the message nearly impossible. E-mail sent through the system becomes almost untraceable. The greatest criticism of such services is that they allow individuals to send harassing or threatening messages without risk of identification.

Employers should also be aware that it is possible to construct an e-mail communication so that it appears to be from someone else. This is commonly called "spoofing." While difficult to do, it is not impossible. Therefore, employers investigating incidents of alleged harassment are advised to consider that the actual harasser is not the person who supposedly sent the harassing message. Furthermore, firing an employee with pornographic files on his hard drive, without further investigation, could be damaging. Another employee may have had access to the computer and downloaded the files, thus incriminating an innocent employee.

For example, at Oracle Corporation, an e-mail message was sent from Adelyn Lee's supervisor to Oracle's CEO, Larry Ellison. The message said, "I have terminated Adelyn per your request." Lee, who had been terminated for poor performance, then used that e-mail message as the basis for a sexual harassment suit. Ellison vigorously denied ever having made such a request, and the supervisor denied ever having sent the e-mail, but the company nonetheless was forced to pay Lee $100,000 to settle her case. Cellular phone records later proved that Lee's supervisor was in his car at the time of the e-mail transmission and could not have been the sender. As it turned out, Adelyn Lee sent the message, but used the supervisor's password to gain access to his computer so that the message would appear to have been sent by him. Lee has since been found guilty of two counts of perjury and two counts of falsifying documents. She was sentenced to one year in jail, and has been ordered to repay the settlement fee.

E-mail As Evidence

Courts are approaching digital data in a way no one could have anticipated, by allowing the discovery in litigation of backup systems consisting of hundreds of thousands of archive tapes. This can be dangerous, because computer users often put messages into e-mail communications that they would never put into writing on real documents. Also, e-mail lasts longer than most users realize. Whenever an employee sends a message over the company's network, two or three copies of the message are stored on file servers before being transferred to archive tapes. Remarkably, e-mail is more permanent than a paper communication. Paper documents can be shredded or discarded, but it is far more difficult to destroy e-mail messages. Even after the "Delete" key is hit, most e-mail systems store messages on a centralized backup file for an indefinite period of time. Mainframe backups also make retrieving e-mail records much easier than retrieving lost paper records.

Employers must understand some of the technical aspects of e-mail communications. Most users of e-mail mistakenly believe that once they hit the "Delete" key, the message has in fact been erased. When a user sends an e-mail message, the user is creating a digital file that is stored on the company's hard drive. The information on the hard drive may be stored for months, or even years. The information remains on the hard drive until the computer runs out of "new" (*i.e.*, unused) space, at which time the computer system will start to fill in ("overwrite") the spaces where the deleted files formerly existed. This can take months, or even years. Alternatively, an employer can "clean out" the hard drive, thus erasing all deleted files.

Employers should beware of two pitfalls when cleaning out a computer hard drive. First, unless an expert performs the operation, the computer files may still exist. Second, employers should not suddenly decide to clean out a hard drive when litigation is looming, or the employer risks being accused of the purposeful destruction of evidence.

The increased role of e-mail in litigation presents serious problems. First, e-mail messages are easier to falsify

than are handwritten or signed documents. Second, lawyers' requests for digital evidence have made the already burdensome discovery process even more onerous for companies, as there are few limits to what lawyers can demand during discovery, and the defendant is usually required to pay for the process of cataloguing and/or sorting its own records. When this process involves retrieving millions of pages of e-mail stored on hard drives or optical disks, the costs can exceed hundreds of thousands of dollars before the case even reaches trial.

More and more employment law cases turn on some form of e-mail evidence. In one case, the plaintiff, a lab technician, used an e-mail message to show that he was wrongfully discharged for his whistleblowing activities. To establish his status as a whistleblower, plaintiff introduced e-mail messages in which he reported "unsafe and illegal practices" to his superiors. The court found that the e-mail messages, coupled with other evidence, provided persuasive proof of wrongful discharge. *Aviles v. McKenzie*, 1992 U.S. Dist. LEXIS 3656 (N.D. Cal. Mar. 17, 1992). Also, in a case alleging sexual discrimination, the plaintiff offered four separate e-mail messages sent by her supervisor, each containing sexually suggestive remarks. *Strauss v. Microsoft Corp.*, 856 F. Supp. 821 (S.D.N.Y. 1994).

Other cases involving e-mail:

- A claim of racial harassment in the workplace was buttressed by a plaintiff who produced evidence of racial slurs contained in company e-mail. *LeSane v. Hawaiian Airlines*, 75 F. Supp. 2d 1113 (D. Hawaii 1999).

- In a suit under the Fair Labor Standards Act (FLSA), to substantiate her claim for nonpayment of overtime compensation, the plaintiff presented an e-mail from her supervisor stating that "I truly want this past weekend to [be] the last one we have to work . . .. I've burnt the midnight oil long enough, just as you have." *Gale v. Levi Strauss & Co.*, 1999 U.S. Dist. LEXIS 9387 (N.D. Ga. Apr. 26, 1999).

- In a retaliation case based on the FLSA, the plaintiff's case turned on evidence of e-mail messages sent by the plaintiff to her supervisors regarding her absence from work. *Angleton v. Beech Aircraft Corp.*, 1997 U.S. Dist. LEXIS 11234.

- In the case of *Vizcaino v. Microsoft Corp.*, 120 F.3d 1006 (9th Cir. 1997), *cert. denied*, 118 S. Ct. 899 (1998), an ERISA case in which the court noted that freelancers were treated differently from employees because, among other things, the freelancers had different e-mail addresses.

- New York Life Insurance Company suspected that one of its employees had violated company policy by charging her monthly commuter pass to her corporate credit card. The employer accused the employee of fraud, even though the employee later claimed that she had sent New York Life a personal check as reimbursement for the credit card expense. The employee was fired, and soon thereafter her supervisor circulated an e-mail message to several employees saying that she had been discharged for credit card fraud. She sued New York Life for libel, and a federal appeals court ruled that she presented enough evidence for trial. *Meloff v. New York Life Ins. Co.*, 51 F.3d 372 (E.D.N.Y. 1995).

Employers should warn employees to use the same care in preparing e-mail messages that they would in drafting a letter on paper. E-mail often lasts longer than messages on paper and is easily forwarded to many other readers. Remind users that a promise made in an e-mail message is just as binding as one made in a letter, and that discriminatory or harassing comments are improper in any form, whether verbally, written on paper, or posted in an e-mail message. Finally, inform employees that e-mail messages should *never* refer to any person's race, color, religion, sex, age, national origin, disabilities, or physique.

Trade Secrets Disclosure

Employers must watch out for angry employees who may post trade secrets on the Internet for millions to see. Recently, a large national corporation sued twenty-one employees for allegedly disclosing company secrets while communicating in Internet chat rooms. The vice president of one of the company's offices is said to be responsible for some of the postings and recently resigned. William M. Bulkeley, *Two Raytheon Employees Resign in Wake of Internet Posting Suit* (Apr. 5, 1999) <http://www.msnbc.com/news/256092.asp>. Access to company trade secrets and other confidential information should be limited to avoid incidents like these.

A trade secret is any information that (1) is secret, and (2) has economic value by virtue of the fact that it is kept secret. Trade secrets may include special formulas, databases, computer software, price lists, customer lists, product designs, business plans, and manufacturing processes. Supplier information (such as key contacts, and customer accounting information), sales forecasts, and financial information, such as budgets, may also be classified as a trade secret. Information that will later be released and become readily known can still be trade secrets until that information is released. (For a more extensive discussion about trade secrets, see Chapter 18 of The 2000 National Employer®.)

While using the Internet, employees can unwittingly or purposely publish valuable trade secrets on public Web sites. With the click of a mouse, an employee can post a trade secret that will be read by millions. The following scenario can happen to any employer with Internet access: Employee Jane Doe intends to send a company trade secret to a client, but hits the wrong keys and mistakenly posts it onto a public Internet message board that is read by thousands of people. By the time she figures out her mistake, the trade secret has been copied and posted to several other message boards. Other confidential information can be disclosed on the Internet as well. Imagine another scenario: Employee Jane Doe is ordering supplies for the company on the Internet. The Internet vendor asks Jane to fill out a customer profile. In so doing, Jane discloses confidential information about Company X's earnings and salary structure.

In some cases, disclosure of trade secrets is a necessary part of doing business. Information that is disclosed to suppliers, customers, employees, or consultants may still be a trade secret, as long as the disclosure is in confidence. Therefore it is essential that employers have a confidential relationship with everyone who will be authorized to have access to information that qualifies as a trade secret. Trade secret law prohibits the recipient of a trade secret from using or disclosing the trade secret without the consent of the owner, if the disclosure is done in violation of a confidential relationship. A disclosure is made "in confidence" when the person to whom the secret is disclosed expressly promises to keep it secret, or it is disclosed in the context of a relationship in which the law will imply an obligation of confidentiality. One way to obtain an express promise not to disclose trade secrets is by means of a signed confidentiality agreement in which the signer acknowledges that the material is secret and promises that he or she will not disclose the information to others.

There are some relationships in which the law will imply an obligation of confidentiality. One such relationship is the employer-employee relationship. In most states, no written contract is necessary to create this obligation, and employees are automatically bound not to disclose or use for their own benefit the trade secrets disclosed to them by their employer, so long as they have notice that the information is confidential. However, when there is no confidential relationship between the owner of a trade secret and someone who learns of it legitimately, the latter is free to use it in any way he or she desires.

Some states, such as California, require that reasonable efforts be made to maintain the secrecy of the information. The company seeking to protect the trade secret will have to demonstrate that it had a program identifying the secret information, a plan for keeping it secret, and a procedure covering persons who may have access to the secret. Efforts necessary to maintain secrecy typically include advising employees of the existence of a trade secret, limiting access on a need-to-know basis, and controlling plant access. These same standards should also apply to information available online. Therefore, employers should identify the

information as secret, and limit online access through passwords or other controls to those who need to access the secret information. In addition, all employees who handle trade secrets should be instructed to include a prominent disclaimer at the top of every message containing a trade secret that clearly labels the message as "confidential" and instructs any inadvertent recipient to return the message immediately. Employers should also consider monitoring access to sensitive information by using software that tracks the identity of persons accessing the information.

Cybertheft

As more companies begin to buy and sell products over the Internet, the risk of employee theft increases. With so many monetary transactions taking place over the Internet, technologically savvy employees will find many ways to engage in cybertheft. Even if the thieves are unsuccessful with their intended victim, they can cause tremendous damage to others. One hacker, who stole credit card data and was rebuffed by the victim company in his blackmail attempts, published the credit card data of hundreds of cardholders on the Internet early this year. <http://cnn.com/2000/TECH/computing/01/10/credit.card.crack.2/
index.html>

E-TRAINING

The Internet has dramatically improved the area of training and education in the workplace by introducing an innovative way to provide workplace training. Employees can now receive training via the Internet on a wide range of topics–from avoiding sexual harassment to balancing the company's bank account. Internet-delivered training, while still a relatively new phenomenon, is expected to become a ten-billion-dollar business by 2002. Luisa Kroll, *Good Morning*, *Hal*, FORBES, Mar. 8, 1999, at 118. It is estimated that more than ninety percent of large American companies have adopted Internet and/or intranet-delivered training programs. David Becker, *Training on Demand* (Jan. 11, 1999) <http:www.techweek.com/articles/1-11-99 /training.htm>. Five of the courses presented at the 1999 Employer are available online at <www.elt-inc.com.>

Internet-delivered training is more convenient than traditional training. Sending employees to training seminars disrupts the workplace and is difficult to organize. Training over the Internet also seems to be more effective than traditional training. Internet-trained employees have been shown to perform better than those who receive traditional training. Internet-delivered training is also less expensive. None of the travel costs associated with sending employees to training seminars are associated with Internet-delivered training. And those travel costs are often significant, with as much as forty cents of every dollar spent on traditional training being spent on travel. *Id.* Internet training may seem expensive at first, but it saves money over the long run. Companies that use Internet-delivered training report impressive cost savings. For example, MCI World-Com claims to have saved $5.6 million last year by using Internet-delivered training instead of traditional training. Aetna claims to have saved $3 million, after software costs, by using Internet-delivered training. Luisa Kroll, *Good Morning*, *Hal*, Forbes, Mar. 8, 1999, at 118, 119.

Discrimination

Employers who implement Internet-delivered training must be careful to avoid discriminatory behavior. The EEOC's *Uniform Guidelines on Employee Selection Procedures* state that the "selection for training" of an applicant or employee must be done without discrimination on the basis of age, race, national origin, disability, or any other protected category. 29 C.F.R. § 1607.2 (1995). Employers must make certain to select employees who receive Internet-delivered training in a nondiscriminatory manner. There is an assumption that younger workers are more comfortable with and capable of using new technology. If an employer were to rely on this assumption and offer Internet-delivered training only to its younger employees, while using in-person training for its older employees, it is likely that this well-intentioned employer would find itself involved in an age discrimination lawsuit. To avoid liability for discrimination, an employer who offers

Internet-delivered training to its employees should offer the training to all employees. If an employee needs extra help learning how to use the Internet-delivered training, such help should of course be given. Also, if a worker refuses Internet-delivered training, even if the training is voluntary, the rejection should be carefully recorded by the employer. If the employer later finds it necessary to terminate the employee for substandard performance and the employee claims to have been inadequately trained, the employer can show that it offered critical skills training, but that the employee rejected the training.

An employer using Internet-delivered training must also make sure to provide reasonable accommodations for disabled employees who may encounter difficulties with such training. The EEOC's *Technical Assistance Manual* lists many examples of reasonable accommodations. Some examples of such accommodations are: providing readers for individuals who have visual impairments or learning disabilities; adding captions to materials that rely on sounds for individuals who are deaf; providing voice-overs for employees who are visually impaired; and offering individualized instruction for employees with mental retardation who may not be able to benefit from Internet-delivered training. On the other hand, the Internet might provide a training delivery vehicle that is especially appropriate for a disabled person who may have difficulties with in-person training seminars.

Negligent Training

A related basis of tort liability that has also gained increased prominence in many jurisdictions during the past decade is the tort of negligent training. Under this theory of liability, an employer is held liable for failing to train or for improperly training an employee. (For a more extensive discussion of negligent training, see Chapter 5 of The 2000 National Employer®.) The digital workplace offers employers greater flexibility to employ innovative employment policies such as telecommuting and working from the home. However, such policies will likely impede, or at least, complicate employers' abilities to supervise and train their workforces as employees become increasingly isolated from the actual work site. Continuous supervision will likely become impossible in light of this expanded job autonomy. Employers will need to devise and implement creative and novel strategies for ensuring that all employees are properly trained and supervised.

The Need To Keep Skills Current

One example of a problem area in negligent training is the technological obsolescence of employee skills. Assume an employee is terminated because his or her skills were outdated and obsolete. The employee could argue that the obsolete skills were the result of inadequate training or opportunities to advance. The employee could also argue that the company's failure to train the employee amounted to discrimination because the employee was a member of a minority, was female, was over forty, or any number of other reasons. In other words, there may be a duty on the part of an employer to maintain training opportunities or at least advise the workforce of the need for training in new technology.

Internet-Delivered Training

Internet-delivered training can actually decrease an employer's risk of being sued for negligent training. Such training seems to be more effective than traditional training. For example, employees at Aetna who were trained over the Internet scored four percentage points higher on training achievement tests than employees who received traditional training. Luisa Kroll, *Good Morning*, *Hal*, Forbes, Mar. 8, 1999, at 118, 119. Internet-delivered training is so effective in part because it allows an employee to learn at her own pace. If she does not understand something, she can study it until she comprehends it. With in-person training, the instructor sets the pace, often leaving the employees behind. In addition, Internet-delivered training provides an ongoing source of education. Anytime the employee has a question, she can consult the Internet-training program for a refresher course. Thus, Internet-delivered training can be seen to actually decrease the risk of negligent-training suits by providing more effective training to employees.

Keeping tracking of which employees have been trained is easier to do when Internet-delivered training is used. An Internet-based training program can record which employee logs on and when that employee logs on and logs off. Thus, an employer can tell if an employee logged off halfway through the training session. An employer who sends its employees to a traditional training seminar may not be aware if an employee walks out in the middle of the seminar.

With in-person training seminars, it is often hard to determine who actually received the training–employees often forget to sign the attendance lists or the lists may be misplaced or lost. Internet-delivered training programs provide accurate records of all employees who have received training. There is no danger of an employee forgetting to sign an attendance list–when he or she logs on, a record of the training is made. The Internet-delivered training program can also be set to notify the Human Resources office when all employees have received training or to warn the office that several employees have still not been trained. Internet-delivered training makes it easier for an employer to ensure that all employees receive training and thus reduces an employer's risk of being held liable for negligent training.

While Internet-delivered training makes it easier for an employer to track which employees have received training, it also can make it harder for an employer to verify that the employee who claims to have taken the training is the person who actually took it. For example, if Employee X believes he is too busy to sit through a lengthy training session, he may convince Employee Y to log on as Employee X and take the training for him. As there is no face-to-face contact required for Internet-delivered training, Employee X could easily get away with such a scheme. The employer, however, faces potential liability for negligent training if Employee X later causes some harm that can be attributed to inadequate training.

There are several things an employer can do to avoid problems like these. First, an employer can require employees who receive training over the Internet to utilize digital signatures (also called cybersignatures). A digital signature is a digital code that is attached to an electronically transmitted message. The code allows the recipient of the message to verify the identity of the sender of the message. There is also new technology that allows a person to actually write his or her signature on the computer. The sender of a message signs a digitizing tablet. This signature is then compared to the signature in the master template that is stored in the computer database to ensure that it is indeed a valid signature.

Legally Mandated Training Requirements

Federal Requirements: Implementing an effective training method has never been more important. Today, employers must comply with a vast number of training requirements. Some of these training requirements are federally mandated. (For a more extensive discussion of federally mandated training requirements, see Chapter 5 of The 2000 National Employer®.) For example, the guidelines issued by the Federal Occupational Safety and Health Administration (Fed-OSHA) require that training on workplace safety take place. In addition, the Federal Drug-Free Workplace Act (DFWA) requires employers who receive grants from, or enter into contracts with, the federal government to inform their workers about the hazards of drug use and chemical dependency. These employers must establish programs informing workers of the dangers of drug abuse in the workplace, must acquaint them with their company's drug-free policy, and must point out available resources for drug counseling and rehabilitation. Employers covered by DFWA who fail to conduct training may forfeit government grants or be excluded from future government contracts.

It is almost certain that in the near future, federally mandated training requirements like the ones mentioned above will increase as government responds to tighter and tighter budgets by spinning off requirements that respond to perceived societal needs without adding to the federal deficit. It costs the government next to nothing to impose a training requirement, especially if the sanction for failure is a lawsuit brought by an individual rather than a fine to be exacted by an agency at that agency's expense. Garry G. Mathiason and Mark A. de Bernardo, *The Emerging Law of Training*, The Federal Lawyer, May 1998, at 25.

The failure to comply with federally mandated training requirements can bring serious consequences, including the loss of government contracts, loss of licensing, and claims for damages from job candidates and current employees. The stakes are very high.

State Requirements: In addition to federally mandated training requirements, many state laws require training. (For a more extensive discussion of state-mandated training requirements, see Chapter 5 of The 2000 National Employer®.) For example, some states require employers to train employees about sexual harassment. Some of these states currently require only that certain occupational groups be trained. Only Connecticut and Maine require private employers to provide sexual harassment training. Other states provide lesser obligations with regard to sexual harassment training. California and Illinois require private employers to distribute information about sexual harassment under certain circumstances. In addition to sexual harassment training, a number of state workers' compensation laws require safety training. These laws are in addition to occupational safety and health requirements already noted.

Settlement, Judgment And Consent Decree Requirements: Workplace training can also become mandatory as the result of the settlement of a lawsuit, or, if the state or federal government has brought suit against the employer, as part of a negotiated "consent decree." For example, in *EEOC v. Sears, Roebuck & Co.*, No. 94-C-0753 (E.D. Wis., Dec. 26, 1995), the EEOC, on behalf of eight former workers, sued Sears for sexual harassment, constructive discharge, and retaliation. As part of the court-approved settlement of the lawsuit, Sears agreed to provide sexual harassment training for two years.

Given the tremendous amount of required workplace training, it is crucial for an employer to utilize the most effective form of training available. Internet-delivered training has proven to be an effective form of training and can help employers deal with the enormous task of complying with the vast array of mandatory training requirements.

Implied Training Requirements

There are many training requirements that while not mandated, are implied. (For a more extensive discussion of implied training requirements, see Chapter 5 of The 2000 National Employer®.) For example, an employer who does not provide training regarding workplace violence faces potential liability from injured parties. Thus, there is an implied requirement that employers train employees in how to spot the signs of incipient workplace violence and how to prevent violence in the workplace. In addition, if an employer does not train an employee and provide that employee with the skills to perform the job, an employee who is later discharged for poor performance can sue the employer for failing to train him or her in the necessary job skills. Thus it can be said that there is an implied requirement that employers provide skills training to employees. Internet-delivered training is an effective and efficient way for an employer to make sure that these implied training requirements are satisfied.

While most states do not require employers to provide sexual harassment training, two recent United States Supreme Court cases have made such training an implied requirement for all employers across the country. In *Faragher v. City of Boca Raton*, 524 U.S. 775 (1998), and *Burlington Indus., Inc. v. Ellerth*, 524 U.S. 742 (1998), the Supreme Court stated that an employer is strictly liable under Title VII for any gender-based harassment by a supervisor that results in a tangible job detriment. If the harassment does not result in a tangible job detriment, the employer is still strictly liable. However, in those circumstances the employer can raise an affirmative defense. It can show that (1) it used "reasonable care" to prevent and correct any harassment and (2) the employee "unreasonably" failed to complain. With these two decisions, the Supreme Court sent a clear message: The failure to train supervisors adequately regarding all appropriate aspects of sexual harassment creates Title VII liability and may deprive the employer of its best defense.

Lower courts have expanded the rationale of the two Supreme Court cases to situations involving race and national origin harassment and will likely expand it to all forms of harassment, including age and disability

harassment, and retaliation. *See, e.g.*, *Allen v. Michigan Dep't of Corrections*, 165 F.3d 405 (6th Cir. 1999) (race); *Gotfryd v. Book Covers, Inc.*, 1999 U.S. Dist. LEXIS 235 (N.D. Ill. Jan. 7, 1999) (national origin). Thus, employers should now consider training regarding all forms of harassment to be an absolute necessity.

Given these new implied training requirements, it is more crucial than ever for an employer to utilize the most effective form of training available. Internet-delivered training is one of the most effective forms of training offered today and should be seriously considered by all employers. Moreover, the ability of Internet-delivered programs to track and create an accurate record of which employees have been trained makes it much easier for employers to later prove that all required and implied training requirements have been met.

An Effective E-Training Program

Once a company recognizes the value which can be added to its performance by e-training of its employees, it should take action as follows:

Research the different Internet-delivered training programs and select an effective Internet-delivered training course. Make certain the training is provided by a reputable and certified source. An Internet instructor's background and qualifications must be investigated just like that of an in-person instructor. Ensure that the information in the Internet training course comes from a qualified expert on the issue and is regularly updated.

Evaluate on an ongoing basis the use of the Internet as a training tool. Monitor the Internet-delivered training programs to ensure that they are effective and accurate. An employer should not simply download a training program from the Internet and assume that it is acceptable. Once a program is implemented, get feedback from employees regarding its effectiveness. Make sure the program gives current and accurate information and covers all relevant issues. Information on the Internet often looks good but end up being out of date or inaccurate.

Do not implement an Internet-training program on employment law that records your scores. Many Internet-delivered training programs evaluate how well participants have learned the material by providing pretraining and posttraining tests. While these are helpful in many areas of traditional learning, they can also present a danger for employers. Employment-law-training test scores may provide ammunition to plaintiffs in subsequent lawsuits. For example, in a sexual harassment lawsuit, the plaintiff may contend that the test results of the supervisor who allegedly harassed him show that the supervisor failed to understand what constitutes sexual harassment.

INTERNET HIRING

Employers around the country are finding that using the Internet is an effective and efficient way to find talented employees. Using the Internet has been shown to be more effective than traditional recruiting in that it creates a more targeted pool of applicants. For example, Hewlett-Packard claims that in the past two years, of 6,500 people who applied on the Internet for jobs, 2,100 were given offers. George Raine, *Trolling the Net for Jobs; Web Attracts Growing Number of Lookers, Recruiters*, S.F. Examiner, Feb. 21, 1999, at B-1. This ratio of applicants to job offers is extremely efficient and shows the effectiveness of Internet recruiting. In addition, employers who use the Internet to recruit may be coming into contact with higher caliber applicants. Studies show that Internet users tend to be better educated and more computer-literate than those who do not use the Internet. Steven Bouvet, *Round Up New Employees on the Internet*, HR MAG., Apr. 1998, at 21.

Using the Internet in hiring is no longer something unique to high-tech companies. Employers in various fields understand the benefits of Internet recruiting and are using it to fill a full range of positions. Approximately $105 million was spent for Internet job advertising in 1998 and that figure is expected to conservatively climb to $1.7 billion by 2003. George Raine, *Trolling the Net for Jobs; Web Attracts Growing Number of Lookers, Recruiters*, S.F. Examiner, Feb. 21, 1999, at B-1.

There are approximately four thousand commercial Internet job sites where job seekers can post résumés and employers can search for job candidates. Michael Erskine, *Job-Hunting on the Net; It Can Open Virtual Doors for the Technology-Savvy*, The Commercial Appeal, June 7, 1998, at H2. Companies can also use their own Web sites for recruiting. One study shows that seventy-three percent of companies with Web sites used those sites to list job postings. Kristine A. Hansen, *Cybercruiting Changes HR*, Hr Focus, Sept. 1998, at 13. Companies that do not want to deal with online recruiting themselves can still reap the benefits of Internet-recruiting by employing one of the many traditional agencies that have begun to use the Internet to search for candidates. In addition, employers can conduct interviews over the Internet and can even give full-color, full-motion tours of their facilities to job applicants and potential customers. David C. Wyld*, Bits and Paper: The Emerging Employment Market in Cyberspace*, 16 Am. Bus. Rev. 64 (Jan. 1998).

Employers can also use the Internet to administer proficiency tests to potential employees, including keyboarding, computer programming, data entry, general math, and psychological tests. Whether advisable or not, a private test center may be linked directly to a company's Internet home page and the tests are instantly scored online.

Recruiting

Employers should use the Internet as only one part of the recruiting process. Other recruiting tools are needed as the Internet does not allow the employer a chance to examine an applicant's oral and interpersonal skills. Face-to-face interviews or video-conferenced interviews should always be part of the recruiting process.

It is possible that employers who post job opening on the Internet but do not post job opening(s) in other more traditional forums could open themselves to an adverse impact claim. This is because some groups of applicants are less likely to have computer access, while other subgroups are more likely to have such access. In an adverse impact case, an employment practice that appears neutral on its face can be found to be discriminatory if it has a harsher or adverse impact on a protected class of people (*e.g.*, Hispanics, females, Asians, etc.). The adverse impact analysis is often applied to determine if employment criteria or employee selection processes are discriminatory.

Employers who use the Internet to recruit applicants, but do not use any other recruitment methods, may find that certain racial subgroups are not as well represented in the applicant pool. Statistics show that minorities and women have less access to computers and the Internet. According to one study, whites are three times more likely than blacks to have Internet access. Chris O'Malley, *The Digital Divide*, Time, Mar. 22, 1999, at 86. Thus, a claim can be made that an employer's sole reliance on the Internet as a means of finding applicants has an adverse impact on women and minorities. Of course, for employers in the computer industry, using only Internet job postings is more likely to be defensible, as an employer could then argue that it was only looking for applicants who are familiar with computers.

It can be argued, however, that using the Internet actually reduces discrimination in the hiring process. For example, an employer who hires over the Internet cannot determine how old an applicant is, what race he or she belongs to, or if that person is disabled. In cyberspace, everyone looks the same and thus the potential for discrimination in the hiring process may be less than through the traditional interview process. Using the Internet to find employees can also reduce discrimination by allowing employers to easily target particular groups of people. For example, an employer wishing to increase the percentage of minority employees can target these employees by posting job openings on Web sites devoted to minority applicants such as Black Voices or Asia-Net. An employer wishing to hire more women can target women applicants by posting on Women's Connect Online.

Résumé Gathering & Database

Soon the act of submitting a paper résumé through the mail may be obsolete. Résumés received by employers

may be in digital formats, such as through e-mail, Internet applications or diskettes, or on paper that can be optically scanned and converted into computer files. Some creative employers who must handle large numbers of applicants now set up computer banks and ask applicants to enter their information directly into the computers.

Software innovations have automated employers' résumé gathering, searching, and tracking. Employers can purchase software to search the résumés stored in a computer, thus eliminating the need to have a staff person sort through hundreds of pieces of paper to find the right applicants for the current job opening. The products have various searching and raking capabilities enabling users to pull up applications with specific skill requirements or experience. The software programs generally rank the résumés on the basis of how well each applicant matches the employer's criteria. The search criteria may be developed by the software maker, or developed by the employer using the software.

While this software is helpful, employers should be aware that they may be accused of discrimination if they use it. One résumé search system, the Resumix System, has been challenged as being based on "majority white culture." Employees of Walt Disney Co. filed a lawsuit in 1997 alleging that the entertainment company's use of résumé-tracking software was evidence of a racial bias in hiring. The employees allege that the software program discriminated on the basis of race because the key search terms were words likely to be used by white persons, whereas minority applicants were more likely to use different word choices.

To avoid an allegation of bias due to use of this technology, employers should first develop a written job description and then develop search criteria directly relevant to that job description. Search criteria might include salary requirements, minimum eligibility requirements such as education or job-related skills, abilities and experience, work conditions (travel, shift work, environmental conditions), and functions, duties, and responsibilities that are essential to the position. Using terms that are strictly linked to the essential qualifications for the job helps to avoid use of factors that are irrelevant to an applicant's ability to succeed in the position. For instance, the Disney suit focused not just on the Disney's use of the software but also on the fact that the company used it without having any objective criteria against which to measure each applicant. Because employers need to have control over the search terms used, employers should only use those résumé search systems that can be customized by the user.

To avoid claims like these, employers should use only those résumé search systems that can be customized by the user. Employers should use terms in their search criteria that are strictly linked to the essential qualifications for the job. This helps to avoid the use of factors that are irrelevant to an applicant's ability to succeed in the position. Acceptable search criteria might include salary requirements, minimum eligibility requirements such as education or job-related skills, abilities and experience, work conditions (travel, shift work, environmental conditions), and functions, duties, and responsibilities that are essential to the position.

Unauthorized Workers

The Internet allows workers from all over the world to apply for jobs and thus increases the chance that an employer will encounter an applicant not allowed to work in the United States. One employer recently discovered that the employees he hired were not from Iowa as he thought, but from India. The Indian workers were not authorized to work in the United States and were supplying their talents strictly through the Internet. This employer's hiring actions may have violated the Immigration Reform and Control Act (IRCA), 8 U.S.C. §§ 1324a and b.

Reporting Requirements

Internet recruiting also presents problems for federal contractors who are required by Executive Order No. 11246 to keep records of the people who apply for jobs, including the race and gender of the applicants. Executive Order No. 11246 requires that every federal contractor and subcontractor agree not to discriminate

against any employee or applicant for employment because of race, color, religion, sex, or national origin, and to take affirmative action to ensure that all applicants and employees are employed without regard to those classifications. The reporting requirements are a way to ensure that discrimination is not taking place.

While an employer can often determine race and gender by simply looking at the applicant, Internet recruiting does not normally allow the employer to see the applicant. Thus it becomes more difficult for an employer to gather the required race and gender data. In addition, determining who is an applicant for purposes of the reporting requirements of Executive Order No. 11246 is not easy when an employer utilizes Internet recruiting. For example, if an employer receives five hundred applications over the Internet, but only examines twenty, must it keep records on all the people who sent résumés or only the twenty people who had their résumés examined? The law in this area is lagging behind technology and has not yet been clarified. How your organization handles this process should be reviewed with corporate counsel.

Fraud And Misrepresentation

The risk of fraud and misrepresentation increases when an employer uses the Internet to recruit. It is much easier to falsify documents and information sent over the Internet. For example, when looking at an applicant's transcript online, the employer cannot check an embossed seal to make sure the transcript is authentic. Employers need to remember this and make sure to verify the authenticity of all documents received over the Internet before making a hiring decision.

Employers should also be aware that it is possible to construct an electronically transmitted message so that it appears to be from someone else. However, there are ways for an employer to verify the identity of the sender of an electronically transmitted message. The employer can verify the sender of a message by requiring the sender to use a digital signature. There is also new technology that allows a sender of a computer message to sign his or her name on a digitizing tablet. The signature is then compared to the master template stored in the computer database to check its authenticity.

There is a culture of anonymity on the Internet that actually encourages people to falsify their identities. It is perfectly acceptable in cyberspace never to reveal one's true identity and to sign all Internet communications with an online pseudonym. In cyberspace, a person who never went to high school can present himself as a prize-winning scientist. An employer who hires over the Internet must be aware of this and must realize that an online applicant may not always be who he or she claims to be. Before hiring anyone over the Internet, an employer should meet with the applicant face to face and should require documentation that verifies an applicant's identity.

An employer also must be careful to avoid making any misrepresentations when posting job openings on the Internet. If the job posting turns out to be significantly different from the actual job, that posting can come back to haunt the employer. For example, such a posting can be used to support a plaintiff's false inducement claim. To prevail on such a claim, an employee must prove: (1) the employer misrepresented or concealed a material fact; (2) it knew of the falseness of the misrepresentation; (3) it intended to induce the employee's reliance; (4) the employee justifiably relied on the misrepresentation; and (5) the employee was damaged as a result. *Lazar v. Superior Court*, 12 Cal. 4th 631 (1996); *Hilliard v. A.H. Robins Co.*, 148 Cal. App. 3d 374 (1983); *Huttegger v. Davis*, 599 S.W.2d 506 (Mo. 1980).

How can employers run afoul of laws prohibiting misrepresentations by them? Imagine the following scenario:

> A plaintiff claims she was falsely induced to leave her job and work for Company X. She claims that the employer induced her to work for Company X by promising her that she would be in charge of over fifty employees. The employer claims that this was not a promise, but only a mere suggestion. However, the employee presents a copy of Company X's Internet posting of the position for which the plaintiff applied that clearly states, "Job Responsibilities: supervise over fifty employees."

Assume a second scenario:

> In an effort to save time, a company uses material from its public relations department in its Internet job postings. As this material was created to attract clients, it understandably contains some overstatements and exaggerations in an effort to make the company appear as attractive as possible to clients. A job applicant accepts a position at the company on the basis of the statements in these materials. Upon discovering that some of the statements in the job posting were exaggerations, she sues for false inducement.

Employers should avoid making any exaggerations or misrepresentations in their job postings. While such puffery may help attract clients, it can also be the basis of a fraudulent inducement claim.

Negligent Hiring

The tort of negligent hiring is based on the principle that an employer has a duty to protect its employees and customers from injuries caused by employees who the employer knows, or should know, pose a risk of harm to others. Thus, an employer may be liable for negligence in selecting an applicant for employment when, for example, the employer neglected to contact the applicant's former employers or to check references, and such an investigation would have demonstrated the applicant's violent or criminal background or other indicia of unfitness for the job. *See, e.g.*, *Doe v. Garcia*, 961 P.2d 1181 (Idaho 1998); *Oakley v. Flor-Shin Inc.*, 964 S.W.2d 438 (Ky. Ct. App. 1998); *Wills v. Brown University*, 184 F.3d 20 (1st Cir. 1999); *Kladstrup v. Westfall Health Care* Center, Inc., 701 N.Y.S.2d 808 (Sup. Ct. N.Y. 1999); *Mendoza v. City of Los Angeles*, 66 Cal. App. 4th 1333, 1339-40 (1998). (For a more extensive discussion of negligent hiring, see Chapter 12 of The 2000 National Employer®.)

The ease and speed associated with hiring over the Internet can make an employer rush through the hiring process without checking references and verifying all information supplied by an applicant. An employer who fails to check references or to contact the applicant's former employers dramatically increases its risk of being held liable for negligent hiring. An increased ability to access information in the digital workplace will undoubtedly affect the standard the courts use when determining whether an employee was negligently hired or supervised. As technology continues to develop, employers will have an expanding array of information at their disposal and a corresponding responsibility to check and investigate the information. Employers will be able to access such information without the need for actual physical possession of documents. The information and documents will instead be accessible by computer via a modem.

On the positive side, the Internet offers a solution to the problem of wanting to hire an employee immediately but having to wait for a background check to be completed. Systems now exist for an almost instantaneous background check. For example, a service named PeopleWise performs fifty-state background checks in less than two minutes. (For more information, visit the PeopleWise Web site at <www.people-wise.com>. PeopleWise is an alliance partner of Littler Mendelson)

In addition to the issue of negligent hiring, there is also the tort of negligent retention. Under this theory of negligence, an employer may be held liable for failing to investigate, discharge, or reassign an employee after becoming aware that the employee is violent or otherwise unfit. *Yunker v. Honeywell*, 496 N.W.2d 419 (Minn. Ct. App. 1993); *Hart v. National Mortgage & Land Co.*, 189 Cal. App. 3d 1420 (1987); *Greenfield v. Spectrum Inv. Corp.*, 174 Cal. App. 3d 111 (1985); *Elam v. College Park Hosp.*, 132 Cal. App. 3d 332 (1982). In larger corporations, where individuals get transferred from department to department, there may be information maintained electronically that could indicate that an employer was negligent for retaining an individual or for not taking appropriate protective or disciplinary steps. An example would be an employee with aggressive or violent tendencies who sends anonymous, threatening e-mail messages to others in the department and is then transferred to another department, where the activity starts anew. The employee eventually is transferred to a third department, where the e-mail messages begin again. This kind of behavior might escalate into an assault or even a homicide. In hindsight, the company could have set up a computer program that traced the source of the threatening e-mail messages to the current assignment of the employee. Indeed, this would probably be viewed as a relatively simple and inexpensive precaution. By failing to use the available technology and digital information, the company could find itself liable for failure to provide a safe work environment and for negligent retention.

Employers must be aware of what information is stored about employees and how that information can be used to avoid negligent retention problems. A standard computer program that contains disciplinary information would help to avoid negligent retention claims. (For a more extensive discussion of negligent retention, see Chapter 12 of The 2000 National Employer®.)

It is advisable for employers to train one employee to access all relevant information available through the digital workplace concerning potential and existing employees. The employee must be instructed on what information is restricted and not accessible without the subject's prior approval. Employers must be aware that obtaining information on potential employees from the information superhighway carries the risk of invasion of privacy and should be done only after thorough consideration and investigation of this issue.

Employment Status

Federal and state laws that protect workers and regulate the relationship between a business and a worker generally apply only to employees, not to independent contractors. Also, employers generally do not maintain benefits for independent contractors. Thus, whether someone is hired as an independent contractor or as an employee is a very important fact with important implications. *See, e.g.*, *Vizcaino v. Microsoft Corp.*, 120 F.3d 1006 (9th Cir. 1997), *cert. denied*, 522 U.S. 1098 (1998) (employer owed millions of dollars to employees who were denied employee benefits because the company misclassified them as independent contractors). (For a more extensive discussion of the implications of independent contractor status see Chapter 28 of The 2000 National Employer®.)

An employer who posts jobs on the Internet must be specific about whether an independent contractor or an employee is being sought for the position. The job posting creates a record that may be used as evidence in a later dispute about employment status.

Privacy Concerns

Companies that receive résumés over the Internet face serious potential legal challenges if these résumés are shared with other companies. A job seeker assumes that the résumé he or she submits to a company will be read only by that company. Given the ease with which information can be shared over the Internet, some employers may be tempted to share résumés with other companies. Other employers may be tempted to sell résumés to online recruiting services. However, sharing a résumé with another company or selling it to a service may violate the privacy rights of the person sending the résumé. Imagine the following scenario:

> John sends his résumé over the Internet to Company X while he is still employed by Company Y. Company X receives the résumé and is impressed by John's qualifications. As Company X is not hiring at the moment, the hiring manager forwards the résumé to her friend at Company Y. The hiring manager at Company Y is shocked and dismayed to find that one of its brightest employees is looking for another job. Company X likely violated John's privacy rights by sharing his résumé with Company Y. Whether John would be able to prove that his privacy rights were violated depends on the circumstances of the case. For example, if he had also posted his résumé on a public Internet job posting Web site, it could be argued that he no longer had an expectation of privacy in his résumé. If John sent his résumé only to Company X, it is more likely that he would be considered to have an expectation of privacy with regard to his résumé and that Company X would be held liable for violating his privacy rights.

INTERNET-INDUCED JOB ELIMINATIONS AND TERMINATIONS

The Internet is increasingly playing a role in employee terminations. Employers are finding it necessary to terminate employees who abuse the Internet at work and employees whose jobs have been eliminated by the Internet. Employers are also finding they may have to terminate employees who cannot adequately use today's technology. Before termination decisions are made, employers must remember that technology used in the workplace creates a record that can be used against the employer. Computer users leave a cybertrail that discloses what they have done and where they have gone in cyberspace. This cybertrail can be used as evidence against an employer in a lawsuit brought by an employee who claims unjust termination.

Termination For Improper Internet Use

Personal use of the Internet by employees during work hours is becoming a growing problem. It is likely that more employers will find it necessary to terminate employees who continually use the Internet for personal reasons during work. Employee use of the Internet for nonwork-related purposes is a significantly larger problem than is perceived by most employers. One study found that twenty-four percent of the time employees spend on the Internet at work is nonwork-related. David Plotnikoff, *Work, the Web & the Watchers* (Oct. 10, 1998) <http://www.mercurycenter.com/premium/front/docs/workweb10.htm>. This number may be low and is increasing with employee access at work to e-commerce.

The Seriousness Of The Problem

If they are not doing work, what are employees doing on the Internet? One study found that in sixty-two percent of the companies surveyed, employees were accessing sexually explicit sites on the Internet. *Id.* Another study found that in every company surveyed, employees were using their work time and employer-paid Internet access to search for other jobs. Lura K. Romei, *Trust, but Verify. . . . (Employees' Internet Use)*, Managing Off. Tech., Aug. 1997, at 7. General news sites, sexually explicit sites, and investment sites are the most popular nonwork-related sites visited by employees. *Over 24 Percent of Employee Time Online is Non-Work Related*, Work-Group Computing Rpt., Aug. 17, 1998 at 3.

The problems for employers of unauthorized use of e-mail and the Internet are not academic concerns. At the end of November 1999, the New York Times fired more than twenty employees for sending "inappropriate and offensive" e-mail messages. <http://washingtonpost.com/
wp-serv/wplate/1999-12/01/ 1701-120199-idx.hmtl> In September 1999, Blue Cross & Blue Shield of Michigan fired seven employees for misusing the company's e-mail system by sending pornographic material and sexual jokes. <http//:www.freep.com /tech/email11_20000211.htm> And Xerox fired forty employees after electronic monitoring revealed that the employees were using

their office computers to visit pornography, gambling, and shopping sites on company time. <http://cbsnews.com/now/story/0,1597,157486-412,00.shtml>

Employee use of the Internet for nonwork-related purposes is inappropriate, but understandable. One commentator compared the Internet situation to giving employees a television set with twenty thousand channels, only seventeen of which are related to company business. In such a situation, the employer can hardly be surprised when the employees are caught watching "Days of Our Lives." Mark Nacinovich, *Web Waste: When Employees Surf the Net*, Accounting Tech., May 1998, at 59.

A new service that actually pays people to surf the Internet will doubtlessly increase the incentive for employees to misuse time at work. This service pays people fifty cents for every hour they surf the Internet so long as they allow a Viewbar with advertisements to remain on the bottom of their browser window as they surf. Kathleen Ohlson, *Pay to Play: New Service Pays Users to Surf* (Mar. 30, 1999) <http://www.computerworld.com/home/news.nsf/all/9903302getpaid>. An employee can easily sign up for the service from her company-provided computer. The whole process takes two minutes and no questions are asked regarding whether one is signing up for the service from a company computer. When an employee gets paid to surf the Web at work, not only are issues of decreased worker productivity implicated, but double recovery issues are also raised. If an employee is being paid by her employer to work a certain number of hours and she is using that time to earn money from another source, that employee is exploiting her position with her employer and is probably violating company rules.

The Burden Of Netsurfing

Employee use of the Internet for nonwork-related purposes is troubling for several reasons. First, employees who are using the Internet for personal reasons often use up valuable bandwidth by downloading entertaining video clips or other documents and programs. This clogs up the system and makes it more difficult for others to use the Internet efficiently. Second, Internet use for nonwork-related purposes costs companies money. The loss of productivity is easy to calculate. For example, if fifty $20-per-hour employees spend just one hour of work time per day surfing the Internet for nonwork-related purposes, the company loses $1,000 per day in worker productivity. According to one study, when the Starr report on the proposed impeachment of President Clinton was posted on the Internet, so many employees spent company time reading it that more than $450 million in productivity was lost. David Plotnikoff, *Work, the Web & the Watchers* (Oct. 10, 1998) <http://www.mercurycenter.com/premium/front/docs/workweb10.htm>.

Personal use of the Internet during work hours also leads to increased risk of liability for the company. An employer can be held liable when an employee uses the company's Internet access facilities for unlawful or inappropriate purposes.

Thus, personal use of the Internet during work hours is a significant problem that may very well cause an employer to terminate an employee. Employers should stress in their policies that improper use of the Internet and all other workplace technology is strictly prohibited and will not be tolerated. (Sample provisions that can be included in an Internet-use policy are at the end of this chapter. A sample policy regarding all kinds of technology in the workplace, such as e-mail, voicemail, and the Internet, can be found in this Chapter.

An employer who terminates or disciplines an employee for inappropriate use of the Internet must make sure that the action is not discriminatory. Consider the following scenario:

> John, a stellar employee, and Jane, an employee with performance problems, both misuse the Internet during work. As John's performance at work is so impressive, the employer assumes that John's misuse of the Internet is not affecting his work performance. Thus, the employer does not terminate John. The employer does, however, terminate Jane because it believes that an employee who is performing poorly should not be surfing the Internet during work hours. Jane sues the employer, claiming that she was terminated, not because she misused the Internet, but because she is a woman. She uses the fact that John was not terminated even though he too misused the Internet, to support her claim that she was terminated on the basis of her sex.

To avoid problems like these, employers must make certain to apply rules regarding Internet use at work consistently.

Netting The NLRA

An employer also must make sure that a termination for improper Internet use does not violate the National Labor Relations Act (NLRA). In a recent case, an employer was found to have violated the NLRA when it fired an employee for e-mail-related misconduct. *Timekeeping Sys., Inc.*, 323 N.L.R.B. 244 (1997). In that case, an officer of the company sent an e-mail announcing changes to the company's bonus system and invited employees to share their views regarding the changes. One employee sent a detailed e-mail message to his fellow employees criticizing the changes. When the employer found out about this e-mail, it demanded that the employee write a memorandum stating that he had behaved improperly. The employee refused to do this and was terminated. The National Labor Relations Board held that the termination violated the NLRA because the employee had engaged in concerted

activity when he used the e-mail system to enlist support for his opposition to the changes in the bonus system. A case like this one is not restricted to e-mail and could easily arise in other contexts. For example, an employee could post his opposition to company policy on Internet message boards or in Internet chat rooms. An employer wishing to terminate an employee for such conduct must make sure the termination would not violate the NLRA.

Another issue employers face is inappropriate use of the Internet by an employee on personal time. Can an employer discipline or terminate an employee for using the Internet in an inappropriate manner or in a manner inconsistent with the interests of the company if that use occurs away from work during the employee's personal time? Imagine the following scenario:

> A teacher in a private school operates an X-rated Web site from his home. He never mentions the site at work or accesses it from his employer's computers. His students learn of the site and spend hours accessing it from their home computers. The school claims the Web site constitutes conduct inconsistent with the interests of the school.

Does the school have a legitimate interest in terminating the teacher or would such a termination be a violation of the teacher's right to privacy? One's right to privacy has been understood to include the right to conduct personal activities without observation, intrusion, or interference. *See, e.g.*, *Hill v. National Collegiate Athletic Assn*., 7 Cal. 4th 1, 35 (1994). Would the school be interfering with this right by terminating the teacher for operating a Web site during his personal time? The answers to these questions are not clear, but would likely be decided through a balancing test. The employee's right to privacy (constitutional or common law) would be weighed against the school's interest in its image and protecting the students it serves.

In order to avoid problems stemming from Internet abuse, consider using blocking or monitoring software to decrease the risk of improper use of the Internet by employees. Create an Internet policy that clearly sets out what is proper and improper use of the Internet at work. This is more than an e-mail and voicemail policy. It addresses the unique features of the Internet. (At the end of this chapter are some sample provisions that can be included in an Internet policy.)

Internet Elimination Of Jobs

Many jobs are becoming unnecessary as the result of advancements in technology. The Internet has displaced many workers because jobs that once had to be performed by a person can now be performed by the Internet. For example, an architecture firm that used to send all blueprints to clients via an in-house delivery department now can send blueprints directly over the Internet. Thus, the delivery department employees are no longer needed.

In addition, as companies rely more on the Internet to sell products, fewer salespeople are needed. Customers buy directly from the Internet and disintermediation results. Catalog retailer Lands' End announced early in 1999 that it planned to lay off almost ten percent of its salaried employees in an effort to emphasize Internet retailing. Wired News, *Lands' End Firings Linked to Net* (Jan. 12, 1999) <http://www.wired.com/news/news/business/story/17287.html>. Some companies such as Egghead Software have moved their entire business to the Internet and sell all products online. Thus, it is clear that the Internet is causing some jobs to become less needed or completely unnecessary. Employers who terminate employees because the Internet has usurped their positions must make certain they terminate employees in a nondiscriminatory manner. For example, if half of the sales positions are being cut, employers must make certain that they are not terminating only older salespeople.

An employer with a unionized workforce will face additional problems when it seeks to terminate employees rendered unnecessary by the Internet. What can be done about displaced or replaced union workers? Can they be terminated without violating the collective bargaining agreement? Must they be placed in other departments? Collective bargaining agreements often have technology clauses that define what will happen within a company with regard to technological change. As Internet use in the workplace continues to increase, more technology clauses will include specific instructions regarding how a company is to deal with changes brought about by the Internet.

When a collective bargaining agreement is silent regarding the employer's right to make a particular operating change and the operating change has a significant impact on employees, the employer may be required to bargain with the union regarding that change. *See, e.g.*, *Newspaper Printing Corp. v. NLRB*, 625 F.2d 956 (10th Cir. 1980), *cert. denied*, 450 U.S. 911 (1981). In *NLRB v. Columbia Trib. Publ'g Co.*, 495 F.2d 1384 (8th Cir. 1974), the court upheld a Board ruling that the employer failed to bargain in good faith when a change in the type of machinery used in its plant resulted in the layoff of half of the bargaining unit. Thus, an employer seeking to terminate employees because the Internet has made their positions obsolete may likely have a duty to bargain with the union before making any decisions. An attorney should be consulted before any termination decisions are made. (For a more extensive discussion about the duty to bargain see Chapter 36 of The 2000 National Employer®.)

Internet Evidence In Termination Cases

Employers who use the Internet in the workplace must also be aware that it creates a cybertrail. Records are kept of all Internet transactions, from the e-mail a person sends to the Web sites a person visits. These records remain long after an e-mail is deleted or a

Web site is exited, and they can come back to haunt an employer in a lawsuit. Employees should be reminded that they are not as anonymous in cyberspace as they think they are and that everything said online should be something that employee would feel comfortable saying in person. All employees should be informed about the long-lasting nature of computer communications. Imagine the following scenario:

> In a fit of anger, a manager sends an e-mail message to her supervisor complaining about an employee. The manager writes, "Ever since Jane got pregnant she has been so irritable. I can hardly stand being around her." Later Jane is dismissed for substandard performance. However, she claims she was fired because she is pregnant. Her lawyers subpoena the company computer records. The manager's e-mail is found and the employee wins her case despite the fact that she actually was terminated for poor performance.

In the past, when a manager wanted to vent about an employee, she would pick up the phone or walk into her supervisor's office. Today, it is more likely that she would send an e-mail to complain. E-mails are dangerous because people tend to put less thought into what is said in an e-mail than to what is said in a written letter. Considering the fact that e-mail messages are stored on a company's hard drive long after they are deleted, this lack of thought is an unfortunate mistake.

Also, people say things in e-mail messages or Internet chat rooms that they would never say in person. There is an assumption that one is anonymous in cyberspace and can therefore say anything with immunity. However, one's online identity can easily be uncovered. In addition, once something is said online, the author of the comment has no control over what happens to that message. If a thoughtless comment is made in an Internet chat room, that comment can be posted to millions of other Web sites in moments. Also, powerful search engines make it possible to find anything that has been said in cyberspace. Although one offensive statement posted in an Internet chat room may seem like a needle in a haystack, today's search engines can locate that statement in seconds. Therefore, thought must be put into whatever is said online. Anything said online should be something one would be willing to say in person.

E-mail messages and conversations in Internet chat rooms create a cybertrail that can later be used against an employer in all types of termination cases such as wrongful termination and termination based on race, age, sex, or national origin. While the use of this evidence has been discussed in this chapter in the context of termination cases, it is important to note that such evidence is in no way limited to such cases. It can be used in virtually any type of case against an employer. Employees of all levels must be reminded of this and must think very carefully before sending an e-mail message or making an online statement.

While e-mail and other cyber-evidence can harm an employer, such evidence can also help employers in certain situations. In a recent "reverse sex discrimination" case, an employer, who was accused of firing an employee because he was a male, relied on several e-mail messages to disprove the employee's claim of sex discrimination. *Comiskey v. Automotive Indus. Action Group (A.I.A.G.)*, 40 F. Supp. 2d 877 (E.D. Mich. 1999). The e-mail messages, sent between the male manager who was eventually terminated and the female supervisor who terminated him, were used to prove that the employee was not terminated on the basis of his sex. In the e-mails, the male employee was insubordinate and unprofessional. The employer relied on these e-mails to prove that the employee had behaved in an inappropriate manner that was out of line for management and had been terminated for such behavior.

An employer can also rely on the cybertrail left by employees who visit Web sites at work to prove that it was justified in terminating an employee. Many employers have tracking systems that allow them to monitor employee use of the Internet. These tracking systems provide employers with a list of all Web sites visited by each employee who accesses the Internet. This evidence can be used to prove that an employee terminated for misuse of the Internet was in fact visiting inappropriate Web sites while at work. However, the record can also be used to support a claim that an employer maintained a sexually hostile or offensive work environment by showing that the employees regularly visited sexually explicit Web sites.

Thus, depending on its content, e-mail and other cyber-evidence can harm or help employers. The important point for employers to remember is that such evidence does exist–regardless of whether the "Delete" key is pushed–and often remains in a company's hard drive.

Terminations For Skills Obsolescence

An employer in the digital workplace will face several unique discrimination issues. Some people are afraid of technology and are uncomfortable learning how to use it. Others have poor typing skills that keep them from efficiently using today's technology. Employers who rely heavily on the Internet and other technology to operate their businesses may find it necessary to terminate an employee who cannot use the technology or refuses to learn how to use it.

What action can an employer take when new technology renders the skills of its employees obsolete? The employees will obviously have to be retrained or replaced. This seems simple enough. However, what if one of those employees is age forty or over and absolutely refuses to be retrained? An employer in this situation must consider the possibility of an age discrimination claim. Age discrimination and, specifically, technological obsolescence of employee skills are issues that employers will face in the digital workplace. An employer cannot discriminate against an employee who is forty years of age or older with regard to that employee's

terms of employment. (For a complete discussion of age discrimination and its defenses, see Chapter 6 of The 2000 National Employer®.) Several questions immediately arise in regard to the employer's course of action. Can the employee be replaced with a younger worker who is paid less and is competent in the new technology? Can the company prove that it needs the new technology to be competitive and successful? Could the older worker be moved to an area of the company where the new technology does not apply? Does the company have an obligation to do so?

When faced with these situations, employers must make certain to avoid discriminatory behavior. If several employees are not able to use the Internet, an employer must make sure to treat them equally. If some are terminated for their failure to use technology and others are not, an employer may be accused of discrimination. Also, an employer may wish to offer training to employees who are uncomfortable with new technology. For example, if an employee refuses to use the Internet because he or she is a poor typist, the employer may wish to offer that employee typing training. If the employee refuses the training and later is laid off for lacking necessary skills, few defenses would be available to the employee.

Another potential discrimination issue involves the disabled. Under the Americans with Disabilities Act of 1990 (ADA), an employer must reasonably accommodate an individual with a disability. (For a more extensive discussion of the ADA and the reasonable accommodation requirement, see Chapter 8 of The 2000 National Employer®.) The digital workplace and the accompanying flexibility in work scheduling and placement, including working from home and/or telecommuting, will likely affect an employer's duty to reasonably accommodate. The federal courts are currently split on the issue of whether an employer must consider allowing an employee to work at home as a reasonable accommodation. Telecommuting is discussed in greater detail below.

The law regarding the Internet is still evolving. The rules an employer must follow when terminating someone for an Internet-related reason are not yet fully understood. Before making a termination decision that is related to the Internet, an employer should consult an attorney.

INTERNET-ACQUIRED AND -DISSEMINATED INFORMATION

The Internet has dramatically increased the amount of information available to a company and has made the information incredibly easy to obtain. By simply accessing the Internet, a company opens itself up to an endless stream of information on any topic imaginable. The information available on the Internet is "as diverse as human thought." *ACLU v. Reno*, 929 F. Supp. 824, 842 (E.D. Pa. 1996). And to access that information, all an employee has to do is to go online and punch in a few keywords–within seconds information is on the employee's computer screen. While the search for the correct information can still be frustrating, the potential is overwhelming. Over the next five years the ability to search this ocean of data promises to improve greatly and to enable an employee to literally have the world's knowledge literally at her fingertips.

In addition to affecting the information that comes into the workplace, the Internet has also affected the way that information leaves the workplace. Before the Internet, if a company wanted to distribute information to many people at once, it had to advertise on television or in the newspaper or to send out mass mailings. Today, by hitting a few keys, a company can send out information over the Internet that will reach millions of people in a matter of seconds. A company Web site can be used to disseminate information about the company to many people, including employees, clients, and potential clients.

The flow of information through the Internet has profoundly changed the workplace. This transformation has brought with it several employment law challenges and opportunities. Selected issues are addressed below.

Compliance Information Sites

A company with Internet access can use the vast amount of information available on the Internet to ensure compliance with the innumerable employment and labor laws governing the workplace. Several government agencies have Web sites that offer information such as rules and statutes and seminal court cases. A few of the most helpful sites are listed below:

- U.S. Department of Justice's Web site on the Americans with Disabilities Act-www.usdoj.gov/crt/ada/adahoml.htm
-
- Immigration and Naturalization Service (INS) Web site–www.ins.usdoj.gov/
- National Labor Relations Board (NLRB) Web site–www.nlrb.gov/
- Fed-OSHA Web site–www.osha.gov/
- Equal Employment Opportunity Commission (EEOC) Web site–www.eeoc.gov/
- Department of Labor Web site–www.dol.gov/

In addition to these helpful Web sites, there are many other sites with information regarding employment and labor law. Littler Mendelson's Web site at <www.littler.com> provides up-to-date information on the most vital employment law issues of the day. Employment Law Training Incorporated (ELT) has a Web site at <www.elt-inc.com> that offers information about products and services employers can use to ensure compliance with all relevant employment and labor laws. Lexcom has an informative Web site at <www.lawroom.com> that provides customized answers to specific employment law questions. The Legal Information Institute has a helpful Web site, located at <www.law.cornell.edu/topics/
employment_discrimination.html>, that offers detailed information about employment discrimination.

While the Internet offers much helpful information, employers must remember that information received from the Internet, even if it comes from a government agency's Web site, is not always accurate or up to date. When looking at a Web site, look for the date the site was last updated to see how current the information is. Information from the Internet should not be the sole source of information an employer relies upon when dealing with important employment law issues nor should it be a substitute for legal advice.

Toxic Information

While the Internet can be a source of useful information, not all Internet information is beneficial. Some of it can be quite harmful when it is brought into the workplace. Employees who use the Internet at work often use it to access harmful material. As mentioned earlier, one study found that in sixty-two percent of the companies surveyed, employees were accessing sexually explicit sites on the Internet. David Plotnikoff, *Work, the Web & the Watchers* (Oct. 10, 1998) <http://www.mercurycenter.com/premium/
front/docs/workweb10.htm>. And the Internet offers much more than just pornography. While surfing the Internet at work, an employee can place an order for marijuana, machine guns, or switchblade knives, and can participate in illegal Internet gambling. In addition, an employee can use the Internet to learn how to commit all sorts of crimes, from building bombs to hacking into computer systems.

If an employee accesses this information while at work, the employer may be held liable. Given the volume of illegal and inappropriate information available on the Internet, the situations in which employers can be held responsible for employees' improper activities on the Internet are virtually unlimited.

There are many cases in which sexist, racist, or other offensive e-mail messages sent by an employee at work result in an employer being sued for allowing an offensive or hostile work environment to exist. For example, two African-American employees of a large investment-banking firm recently sued their employer for hostile work environment harassment. They demanded twenty-five million dollars each in damages due to a racist e-mail that was circulated among the white employees. The case was later settled. *Owens v. Morgan Stanley & Co.*, 1997 U.S. Dist. LEXIS 10351 (S.D.N.Y. July 17, 1997) (case later settled). In another case, four female employees sued Chevron for sexual harassment. Chevron agreed to settle the suit for $2.2 million when records of offensive e-mails with titles such as "why beer is better than women" were presented. Michael Rapoport, *E-mail Increasingly at the Center of Workers' Discrimination Suits*, The Daily Rec. (Baltimore, MD), Feb. 20, 1997, at 11.

The Internet has caused an increase in environmental harassment cases like these because it is a source of so much inappropriate and easily obtainable material. An employee who wishes to send sexist or otherwise offensive e-mail messages no longer has to rely on his or her imagination for offensive information to include in the messages. Any number of offensive images or statements can be downloaded from the Internet and sent via e-mail to fellow employees. The employees who receive the images can easily turn around and sue the employer for allowing a hostile or offensive work environment to exist.

Employers can reduce their chances of being sued for hostile or offensive work environment harassment by restricting employee Internet access to pornographic or other offensive Web sites. Blocking software can keep employees from accessing certain inappropriate sites, while monitoring software allows employers to watch how employees are using the Internet. Usually, monitoring software is used to track overall Internet usage, rather than an individual employee's usage.

Employers can also reduce the risk of employees accessing toxic information by implementing an Internet usage policy that clearly sets out what is appropriate and inappropriate use of the Internet at work. Such a policy should clearly state that access to pornographic, racist, and other offensive Web sites is prohibited and that absolutely no offensive material may be downloaded from the Internet at work. (Sample provisions for such a policy are included at the end of this chapter.)

An Internet usage policy not only reduces the chances that an employee will access toxic information, but can also help an employer to avoid liability for hostile work environment claims. In a recent case, a female employee sued her employer for hostile work environment sexual harassment, among other things. The court did not allow her claim to proceed to trial, finding that even if there was a hostile work environment, the employer took "prompt and reasonable corrective steps with respect to these problems . . .." *Spencer v. Commonwealth Edison Co.*, 1999 U.S. Dist. LEXIS 261, *27 (N.D. Ill. Jan. 6, 1999). The court considered the fact that the employer attempted to curb the inappropriate use of company computers by implementing an Internet usage policy and that the employer disciplined employees who inappropriately used the Internet as evidence that the employer took prompt and reasonable corrective steps regarding the alleged harassment. Thus, an Internet usage policy can help an employer prove that it took appropriate steps to prevent or correct a hostile work environment.

Employee Abuses Of Digital Information

Employers should be aware that this new technology can also reduce productivity and may create liability issues. Employee misuse of corporate e-mail for personal purposes wastes company time. Furthermore, one study indicates that over twenty percent of e-mail users have received sexually harassing e-mail. Also of concern is the potential for an employee to abuse an e-mail system in order to perform an illegal operation. An example: a Bank of Boston employee was found to be running a bookie operation over the bank's e-mail system. Employer liability may be increased in other areas as well. Under the tort of "product disparagement," or "disparagement of quality," an employer could be held responsible for a message sent by an employee regarding a customer or a competitor.

The digital workplace holds other hidden traps for employers. For instance, employers may be liable for an employee's use of e-mail to send or receive material that infringes a copyright, such as pirated software. Employers may also be held responsible for employees' use of e-mail to send or receive trade secrets in violation of the rights of the owner of the trade secret, for an employee's use of e-mail to publish defamatory statements or send or receive obscenity or child pornography, and for harassment. Additionally, an employer may be liable for an employee's use of e-mail to make statements or enter into contractual commitments that bind the company to a particular viewpoint or to a contractual obligation.

An employer may be liable for copyright infringement, even if that employer did not actually perform the copying or distributing. Under the theory of contributory infringement, an employer may be liable for infringement committed by an employee if the employer had knowledge of the infringing activity, and induced or materially contributed to the infringing conduct. *See, e.g.*, *Religious Tech. Ctr. v. Netcom Online Communication Servs., Inc.*, 907 F. Supp. 1361, 1373 (N.D. Cal. 1995). Under the theory of vicarious liability, an employer may be liable for an employee's infringement if the employer had the right and the ability to supervise the employee's activity, and had a financial interest in exploitation of the copyrighted materials. *Id.* at 1375-1376.

An employer in possession of improperly obtained software may be accused of copyright infringement. A copy of a software program that cannot be validated by purchasing records might result in an allegation of copyright infringement. This can be caused by software that was brought in from an employee's home, or was created by conscientious employees trying to get a job done more efficiently. Or, perhaps the software is an unauthorized copy created by a well-meaning but misguided cost-conscious manager. A software management program may reduce the risks of counterfeit or copied software. Employers should set guidelines for downloading software and data from online services and the Internet. Employers should also audit personal computers and network machines and should destroy any illegal software they find. Finally, employers are advised to keep a catalogue of all software licenses.

Copyright infringement settlements can be expensive. For example, suppose there is an average of two illegal programs per computer, with an average cost of one hundred dollars, and assume that there are five hundred machines within an organization's headquarters and branch offices. The cost of purchasing legitimate copies of the illegal software might be one hundred thousand dollars. Penalties are usually one to two times the retail value of the illegal software.

Unions And The New Order

The transformation of the American workplace into a digital workplace is creating unique problems for the unionized employer. Problem areas include privacy issues, swiftly changing job roles, skills and duties, different measures of productivity, the need for constant training to keep up with new technology, and the ability of the employer to utilize flexible work relations such as telecommuting. Key union concerns in the telecommuting area are fairness in performance reviews for telecommuters, the level of technical and support available, overtime and other wage-and-hour issues, electronic monitoring and employee privacy, a shift toward using contract personnel for piece work assignments, and the union's ability to continue to represent workers at remote locations.

The union movement is beginning to assert its place in the digital workplace. For the first time ever in an airline union contract, British Airways agreed to provide its U.S.-based employees with five-day advance notification before it will electronically monitor telephone calls and computer entries of reservation clerks and passenger service agents. Similarly, in a union contract signed by Cincinnati Bell, the company agreed to warn employees that it may be monitoring their activities. Monitoring in the Cincinnati Bell contract includes keystroke monitoring and audio monitoring where supervisors listen in on customer-employee conversations. The unions will likely increase their involvement in digital workplace issues as more of the issues emerge as concerns of employees.

What happens when new technology replaces work that was previously performed manually? Will the work created by the new technology be included in the old bargaining unit? What can be done about displaced or replaced union workers? One film-industry employer has faced this problem. The Employer made models of sets to be used in films. The model making was initially performed manually. However, the advent of virtual reality made it more efficient and effective to make the models on a computer. The use of computer technology would require the layoff or replacement of union workers. The issues that arose include the proper definition of the bargaining unit and whether the new work should be done by union employees.

Employers who are aware of these problems may be able to structure the technological change in a way to avoid or minimize

liability. This is not an isolated incident. Employers will increasingly face similar problems. A more complete discussion of the law concerning the unionized workforce can be found in Chapter 35 of The 2000 National Employer®.

Cyberspace Organizing

Unions are increasingly using the Internet as a union-organizing tool. Cyberorganizing is heralding a new era in union organizing. The Internet and the World Wide Web are being used to make information about unions available to employees around the country. (For a more extensive discussion about union organizing in the digital workplace, see Chapter 17 of The 2000 National Employer®.) The AFL-CIO, the SEIU, and most other major unions have home pages on the Internet. These unions use their home pages to post information about union organizing efforts and to target a particular employer as part of a corporate campaign. The AFL-CIO's Executive Paywatch Web site allows employees to compare their salaries with those of the top executives of Fortune 500 companies. In addition, instead of attempting to make house calls or merely sending out mailers, union organizers are able to directly contact employees interested in unionizing via e-mail and postings on the World Wide Web. Employees can also use the Internet to download union authorization cards.

Available Union Information

Numerous *How to Unionize* Web sites exist, complete with information on labor organizing, union election procedures, examples of unfair labor practices, and news about other organizing efforts. Many unions now provide strictly confidential "Unionize Your Workplace" forms for anyone interested in receiving information on organizing a union. Such forms ask for the inquiring employee's address, phone number, e-mail address, type of work, and number of employees. Once completed, these quick and easy forms are sent off to the union with a mere click of the mouse. This new union tactic of using the Internet is an especially effective one in terms of reaching "Gen-Xers."

Employers troubled by the fact that their employees are using company time and company-provided Internet access to obtain union information do have the right to prohibit access to such information during work hours. However, in order to avoid violations, employers must make sure to prohibit employees from accessing any and all nonwork-related information on the Internet, not just union information. Given the newness of computer technology, it is still not clear how the NLRA will be applied to union organizing over the Internet. Until the law becomes clearer, employers should be cautious and consult counsel before making any important decisions.

The NLRA grants employees the right to organize, support, and join labor unions. As more employees gain access to company e-mail systems, employees will undoubtedly use employer e-mail systems for union activity. The NLRB has not yet ruled on how organizers may use employers' e-mail systems. In one NLRB case, the Board held that employers cannot enact policies exclusively prohibiting union e-mail messages. However, the case may have raised more questions than it answered. *E. I. du Pont de Nemours & Co.*, 311 N.L.R.B. 893 (1993). For instance, the administrative law judge in the case raised, but did not answer, the question of whether an employer could ever lawfully prohibit its employees from using its e-mail system to transmit union messages.

On the one hand, the NLRA gives employees the freedom to communicate with one another while on the job site as an essential component of their right to self-organize. On the other hand, under certain circumstances a company may enact a no-solicitation or no-distribution rule prohibiting union soliciting and leafleting. Bans on solicitation during working time in working areas are presumptively valid under the NLRA. However, an employer may not use an otherwise valid no-solicitation rule to discriminate against union activity. Employers possess other rights even in the absence of a no-solicitation rule. For instance, they can fire employees who interfere with their coworkers' productivity, even if the interference is for the purpose of discussing union business. The NLRA does not protect disruption of other employees' productivity. An employer also has the right to prohibit employees from placing nonwork-related notices on bulletin boards. However, the employees' right to discuss self-organization extends to placing notices on bulletin boards when an employer has waived its right of exclusive control over the bulletin board. In other words, once an employer permits employee access to a company board, it cannot thereafter remove notices or discipline or threaten an employee who posts pro-union notices.

Employee rights to organize and to discuss organization with other employees generally do not give nonemployee organizers the right to enter an employer's property to discuss union organizing. Generally, nonemployees may not enter an employer's premises to engage in union organizing except where the employees live and work beyond the reach of reasonable union efforts to communicate with them. This raises the issue that an employer with a very spread-out workforce, perhaps because of telecommuting, might be obligated to give unions the right to reach employees by e-mail.

Organizing By E-mail

E-mail and computer technologies may change all of these rules. Unions increasingly use e-mail as a method of disseminating information. E-mail somewhat resembles the posting of messages on a conventional bulletin board, but differs because nonwork-related e-mail messages are not easily detected. The Electronic Messaging Association estimates that on-the-job Americans send two billion electronic messages each month. While e-mail is a powerful communications tool for companies, it is also a powerful

communications tool for union organizers.

E-mail differs from traditional letters and flyers in several important ways in the union organizing context. Employers are less likely to know of e-mail messages as they pass through the computer system, whereas employers present at the workplace could observe literature distribution, or can readily see notices posted on conventional bulletin boards. Furthermore, e-mail messages do not physically litter an employer's property. This aspect is important, as courts permit employers to ban employees from distributing literature in working areas because such distribution may litter the employer's premises and raise a hazard to production. E-mail does not necessarily pose such a risk to an employer's property. One writer has argued, however, that e-mail poses a different, and equally troublesome, burden on employers. Professor Frank Morris argues that e-mail impinges on the rights of employers even more than the distribution of literature, because e-mail uses employers' hardware, time, and resources, and constantly interferes with work functions. Furthermore, allowing nonwork-related information to pass through company e-mail slows down the entire e-mail system.

Unions increasingly are turning to the Internet as a union-organizing tool. The AFL-CIO, the SEIU, and most other major unions have home pages on the Internet. These unions use their home pages to post information about union-organizing efforts and to target a particular employer as part of a corporate campaign. In addition, instead of attempting to make house calls or merely sending out mailers, union organizers are able to directly contact employees interested in unionizing via e-mail and postings on the World Wide Web.

Employers are taking the initiative in making more easily available to their employees both computers and software for home use, provided at reduced cost. Ford announced earlier this year that it would provide its 101,000 employee-members of the United Auto Workers with a home computer and Internet access at five dollars per month. BNA Daily Labor Report, February 4, 2000, p. A-7. Delta Air Lines followed suit shortly thereafter, indicating it would provide its 72,000 employees with similar hardware and software benefits. BNA Daily Labor Report, February 7, 2000. Not to be outdone, the AFL-CIO announced within the last year a member benefit of access to an Internet service provider at a cost not to exceed $14.95 a month, and computers and software available for member purchase at attractive pricing, with financing.

The Internet is also specifically being used to target white-collar, high-tech sectors such as many Silicon Valley employees. Web sites have been designed to reach out to these employees at technology firms. In particular, AFL-CIO President John Sweeney sees potential for large membership gains among the computer industry's corps of "permatemps"–those employees who are treated as independent contractors and therefore do not qualify for company benefits.

Union organizers have sought union elections in nontraditional areas, such as Borders bookstores. In the Borders case, the NLRB conducted elections in five Borders stores and the union won representation in three of the bookstores. The union won, in part, by using the Internet and e-mail to distribute and communicate their messages to the younger, computer-literate workers at the stores.

How To Protect Against Cyberorganizing

Employer "No Solicitation" and "No Distribution" rules should apply to company e-mail systems. Employers should take care to enforce uniformly the prohibition against *all* nonwork-related messages, or else a court may find that the employer disparately and discriminatorily applied the policy against union activity. This poses an enormous burden for employers, placing high monitoring costs on employers.

An employer could argue that no-solicitation and no-distribution rules should apply to e-mail, because e-mail organizing cannot be confined to nonworking time. Employers may want to consider denying employees access to their employer's e-mail system from home to check for personal messages. Additionally, employers should be sure to reserve the right to monitor employee e-mail, and may want to consider rules prohibiting mass e-mailings. At the very least, employers should consider monitoring any mass e-mailings.

The ease with which information can be disseminated to millions of people over the Internet creates many risks for an employer with Internet access. Employers must be aware of these risks.

E-Distribution Of Personnel Policies

Some employers are taking advantage of new technologies to distribute employee handbooks, personnel policies, and benefits information electronically. For instance, some employers post their employee handbooks on a Web site. Others post their employee handbooks on an internal Web site, also known as the Intranet. Both technologies offer benefits, such as a reduction in copying and production costs associated with producing a traditional employee manual. However, each of these new technologies comes with hidden risks. For instance, how does an employer ensure that each employee reads the manual? How does an employer insure that each employee receives and reads updates? How does an employer preserve previous copies of the handbook? If your handbook is posted on the Web, is there any danger that a competitor may gain inside information about your company?

One of the best ways to post employee handbooks is on an internal Web server. These internal Web sites, or Intranets, enable companies of all sizes to enhance communication within the organizations by distributing company information such as employee

handbooks and training materials. According to one study, nearly ninety percent of all enterprises are currently using Intranets.

The Intranet is a private network generally meant to be used by one employer. The Intranet runs parallel to any other existing network. A company does not have to have access to the Internet to start an Intranet. While there are costs associated with installing an Intranet, benefits include the ability to protect company information from the prying eyes of competitors, and use of an Intranet makes the company less exposed to penetration from an outside hacker. An Intranet does not, however, protect a company from an employee who "hacks" into the Web site and makes changes to the posted policy or handbook.

There are also new software systems that help employers track which employees have accessed the handbook and which ones have not. These same tracking systems enable employers to track employees who have not yet accessed the revised handbook. Of course, access doesn't ensure that the employee read it, but the same has always been true when a large bound book is given to a new employee. One new software system enables selected individuals to post and track policies and procedures for the organization, and allows the rest of the organization to read them.

PRIVACY IN THE DIGITAL WORKPLACE

The developing doctrine of employee privacy and the dramatic expansion of the digital workplace have combined to create one of the most important areas of employment law as we enter the Twenty-First Century. (For a more extensive discussion of employee privacy, see Chapter 21 of The 2000 National Employer®.) We have entered the "Information Age," in which the amount of information that can be obtained about an employee is virtually unlimited. This rapid development of information technology and the mass availability of information have the potential to eclipse an employee's right to privacy in the workplace. For example, the digital manager has the ability to monitor an employee from the time he or she wakes up in the morning, comes to the office, travels to a distant city on a business trip, and returns. The manager has the power at her fingertips to monitor, survey, and search employees' e-mail, voicemail, or personal computers.

The critical question raised by the power of electronic monitoring is how to balance an employee's right of privacy against the availability of tremendously valuable information. An employer must address this delicate balance and establish rules and regulations regarding its formation. The alternative is a dramatic increase in litigation costs. Indeed, during the past decade we have seen an increase of three thousand percent in the number of privacy lawsuits. It is our goal here to focus on current law that provides guidance to employers concerning the use of technology and the protection of individual privacy.

Monitoring Employee Internet Use

Many employees do not realize that Internet "surfing" leaves a digital trail. For example, an Internet provider may automatically record each individual's use of Web sites, news groups, and e-mails. This record of the sites visited by employees may be used in litigation against the employer: In one case, evidence of repeated employee visits to sexually explicit Web sites was used to show that the employer maintained a sexually permissive work environment.

Employers may wish to purchase software that denies access to any sites containing potentially offensive images. Such software can also be used to maintain employee productivity by denying access to other nonwork-related sites. However, it is still possible for employees with modems to install their own Internet access software. Employers should therefore consider purchasing software to alert them to any Internet access software.

When an employee surfs the Internet, he or she leaves a cybertrail that allows an employer to track exactly where that employee has gone in cyberspace. A user's Web browser creates files that record all of a user's interactions. There is also a file called a cache file that can keep copies of any pictures that have been downloaded. Many employees feel their privacy has been invaded when they discover that their every move on the Internet has been recorded.

Employers who choose to monitor employee use of the Internet must be careful to avoid violating the privacy rights of employees. The single most important point for employers to remember regarding privacy in the workplace is the need to reduce employees' expectations of privacy in the workplace.

This year, a court found that an employee did not have a reasonable expectation of privacy with regard to any of his Internet activity at work. *United States v. Simons*, 2000 U.S. App. LEXIS 2877 (4th Cir. Feb. 28, 2000). Thus, his rights were not violated when his employer searched his computer workstation and found illegal pornographic images. The court found that the employee had no expectation of privacy because the employer had a policy that clearly stated the employer would monitor Internet use.

This case illustrates the importance to a company of drafting, promulgating, and enforcing a clear Internet policy. Such a policy must explicitly state that the employer has the right to monitor all computer and Internet use and that the employee has no expectation of privacy with regard to his or her computer use or computer communications at work. (At the end of this chapter are sample provisions that can be included in an Internet policy.) The policy should then be disseminated to all employees and the employer should have training programs explaining the policy. Employees should be reminded often that the employer has the right to access e-mail and

Internet files.

Monitoring Employee E-mail & Voicemail

Employers are starting to take advantage of new technologies for surveillance and electronic monitoring of employees. Employers now have the technology to monitor an employee's conversations, computer keystrokes, performance standards, and whereabouts on a minute-by-minute basis. An employer's rights in this area are, however, limited. The same federal and state laws discussed in the preceding section with regard to searching voicemail and e-mail message systems apply equally to monitoring. Moreover, some states, including California and Connecticut, have laws forbidding employers from surveilling and monitoring employees in certain circumstances. (See the Reference Table at the end of Chapter 21 of The 2000 National Employer®.)

The interplay of technology and individual privacy is well illustrated by a federal court case in Pennsylvania, where the court found that terminating an employee for "inappropriate and unprofessional comments . . . over [the company's] e-mail system" constituted proper grounds for dismissal. *Smyth v. Pillsbury Co*., 914 F. Supp. 97, 101 (E.D. Pa. 1996). The employee had exchanged e-mail with his supervisor that contained offensive references and threats concerning the company's sales managers. Specifically, the plaintiff threatened to "kill the backstabbing bastards," and referred to the company holiday party as the "Jim Jones Kool-Aid affair." *Id.* at 98 n.1. The supervisor forwarded the e-mail to company executives, who then read all of the plaintiff's e-mail messages and terminated the plaintiff. The employee sued, alleging that the interception of his e-mail messages violated his right to privacy under Pennsylvania law. The court disagreed, and concluded that an employee has no reasonable expectation of privacy in e-mail communications voluntarily made to a supervisor over a company-wide e-mail system, regardless of any assurances from the employer that e-mail messages would remain confidential and privileged. Furthermore, the court noted that, "The company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighed any privacy interest the employee may have in those comments." *Id.* at 101.

In another case, a Los Angeles employer was charged in a class action suit with violating several of its employees' privacy rights by eavesdropping and intercepting the employees' e-mail messages. *Flanagan v. Epson Am.*, Case No. BC-0670-36 (L.A. Sup. Ct. 1990). Apparently, such monitoring is not uncommon. According to a report by the American Management Association, sixty-three percent of midsize to large companies conducted some form of electronic surveillance, as of January 1999. The Wall Street Journal reported on February 28, 1995, that a 1993 survey of 301 employers conducted by Macworld found that twenty-two percent of the employers surveyed admitted to monitoring employee voicemail, e-mail, or computer files. Moreover, many of those employers engaged in the monitoring without obtaining employee consent, and, in many cases, without any employee knowledge of the monitoring whatsoever.

A suit filed in a federal court in Rochester, New York, serves as an example of the type of problems employers can expect if they do not address the monitoring issue and may help define the scope of an employer's right to monitor employee voicemail. The suit, brought by a former manager of a McDonald's restaurant, alleged that McDonald's violated the Electronic Communications Privacy Act and the Omnibus Control and Safe Streets Act, both discussed below, by monitoring and seizing his voicemail. The manager was having an affair with another employee of McDonald's, during which the two employees left each other private "aural" messages on each other's voicemail. A coemployee accessed the two employees' voicemail boxes and transmitted the sexually explicit messages to the voicemail of the owner of the restaurant; the coemployee also made tape recordings of the messages and played them to the manager's wife. In the suit, the former manager alleged he was told his voicemail was private and that only he had the code to access the voicemail. He also alleged that he was told the use of voicemail was not limited to work-related messages. The manager further alleged he was fired when he complained to this boss about the "invasion of privacy" and sought punitive damages. Pamela Mendels, "*$2M Suit in Sweet Nuthin Eavesdrop*," N.Y. Newsday (Jan. 20, 1995) at A4.

The sample policy at the end of the chapter on voicemail anticipates many of the issues in the above example. The sample policy states that voicemail is the property of the employer and is not to be used for personal matters. However, even with such a policy, an employer should generally not electronically surveil or record employee conversations without advance notice to and consent of all parties involved, a strong, legitimate business purpose for such activity, and advice of counsel. (A sample notice to employees regarding access and monitoring is included at the end of this chapter.) The potential civil and criminal penalties for violations are quite serious and appear to reflect an overall orientation against surveillance and recording activities except under color of law or as necessary for communications utilities' rendering and maintenance of services. *See, e.g.*, 18 U.S.C. §§ 2511(2)(a)(ii); 2702(b). Notably, communications at public gatherings or formal proceedings open to the public are excluded from these requirements, as are any other circumstances in which a party may reasonably expect that the communication may be overheard or recorded. Limited exceptions apply to public utilities providing communication services and facilities under both federal and state law.

Employers who do choose to use monitoring devices must ensure that the devices do not inadvertently pick up nonemployees. For example, cameras designed to detect theft in a dressing area of a department store may inadvertently be positioned in a way that exposes individuals changing clothes in his or her private dressing room. Under such circumstances, employers might be charged for the inadvertent violation of the individuals' right to privacy. (In California, such surveillance could be a crime. Cal. Penal Code § 647(k)(1).) Accordingly, employers must give careful consideration to the full consequences of the use of electronic monitoring technology in their workplace. Controls should be instituted to protect against the overbroad use of monitoring equipment.

Customer Service Monitoring

In today's increasingly competitive economy, employers must sometimes monitor their employees in order to maintain and improve productivity. For instance, employers often monitor telephone conversations of airline reservation clerks, customer service personnel, and telephone operators. Employers may monitor these calls in different ways, including telephone call accounting monitoring (where the number of calls per hour and the length of each call are recorded), and service observation monitoring (where supervisors listen in on calls).

The rules on monitoring telephone conversations vary from state to state. For instance, under California law, telephone monitoring is prohibited unless *both* parties consent. Generally, the nonemployee user is advised at the beginning of each telephone call that the call may be monitored. Cal. Penal Code § 631.

In other states, however, telephone monitoring is legal as long as the monitoring is done for a legitimate business purpose. An employer may monitor by extension phone an employee's business-related calls as long as the employer offers a legitimate business reason that justifies such monitoring. *James v. Newspaper Agency Corp.*, 591 F.2d 579 (10th Cir. 1979). In *James*, an employer had the telephone company install a monitoring and recording device on the business line, so that a manager could monitor business calls made by employees to address "the concern by management over abusive language used by irate customers when called upon to pay their bills, coupled with the possible need to give further training and supervision to employees dealing with the public." *Id.* at 581. The court found that the monitoring was legal, in part because both the employees and the customers were aware that their calls were monitored, and in part because the monitoring was done for a legitimate business purpose. Although the *James* case dealt primarily with extension monitoring by supervisors, the practice of recording employees' conversations with customers is now generally determined to be within the bounds of accepted business practice. *Briggs v. American Air Filter Co., Inc.*, 630 F.2d 414, 418 (5th Cir. 1980). When customers complain about a possible invasion of privacy, courts have noted that even though it may be more difficult to justify recording the customer's responses, it would be extremely difficult for a business to gauge the performance of its employees without hearing both sides of the conversation. *Id.* Additionally, courts are generally more sympathetic to employers' arguments when the access to monitoring is strictly limited to quality management supervisors. *See, e.g., O'Sullivan v. NYNEX Corp.*, 426 Mass. 261 (1997).

Searches In The Digital Workplace

One major concern in the digital workplace involves efforts to search and retrieve voicemail, e-mail, and similar electronically stored messages. Employers often have a legitimate need to search an employee's e-mail or voicemail messages. For example, one company in California searched an employee's e-mail messages for evidence of trade secret violations. The search was prompted by the employee's defection to a major competitor. The company suspected that the former employee had been using the company's e-mail system to transmit trade secret information to the CEO of the major competitor. The company's search allegedly confirmed their suspicion. *Borland Int'l Inc. v. Gordon Eubanks* Case No. 123059 (Santa Cruz Sup. Ct.).

Although employers often have a legitimate need to conduct a search, cautious employers must be aware that their actions may violate an employee's right to privacy. Several federal and state court decisions, described below, illustrate the concerns in this area.

The Fourth Amendment's Proscription Against Unreasonable Searches & Seizures

A review of cases involving the Fourth Amendment's proscription against unreasonable searches and seizures is helpful in formulating a policy in this area. The Fourth Amendment with its proscription against unreasonable *governmental* searches and seizures does not directly relate to the *private* workplace. However, it is an excellent starting point for the analysis of workplace privacy. Several of the doctrines that have been developed in the area of privacy arise out of litigation with regard to the Fourth Amendment and its applications. Increasingly, the tests articulated by the Supreme Court in various Fourth Amendment cases are being used in the context of the private workplace.

The Supreme Court in *O'Connor v. Ortega*, 480 U.S. 709 (1987), established a "reasonableness test" to balance a public employee's expectation of privacy in his office against an employer's right to conduct a reasonable search under the circumstances. By adopting this test, the Supreme Court sought to balance the employee's privacy expectation against the employer's legitimate business needs. If the employer has a legitimate need for the information and reasonably limits the scope of the search, the search will likely be regarded as protected and reasonable. A public employer may further increase its discretion to conduct searches by lowering its employees' privacy expectations. One way to accomplish this goal is to notify employees that they and their possessions may be subjected to searches at work. *Id.* at 717.

Private employers are not constrained by the Fourth Amendment. Nevertheless, employers are advised to follow the dictates of *Ortega* and the Fourth Amendment. The reason for this caution is simple. Although several state legislatures and courts have created privacy rights for employees in the private sector, that law is largely unsettled and in flux. For example, the California Supreme Court confirmed that California's constitutional right of privacy applies to private entities. *Hill v. NCAA*, 7 Cal. 4th 1 (1994). Before the *Hill* decision, conflicting standards existed for assessing California's constitutional right of privacy and a question existed as to

whether the right applied in the private sector. Through its decision in *Hill*, the California Supreme Court described the standards for analyzing the employer's "need to know" versus the prospective or current employee's right to privacy. (See further discussion on *Hill* in Chapter 21 of The 2000 National Employer®.)

Several states across this country are still waiting for a decision like *Hill* to help clarify their own privacy law. California has traditionally been a leader in the area of employment law developments so this decision may be a harbinger of things to come for employers in other states. However, until the law is clearly developed, employers should ensure that their searches meet the high standards set by *Ortega* and the Fourth Amendment.

Based on the dictates of *Ortega*, in general, searches should be based on reasonable suspicion or legitimate business needs and limited in scope to that necessary to achieve their purpose. Further, employers should endeavor to reduce their employees' expectations of privacy. This can be accomplished in several ways. Written authorization could be obtained from the employees before the search. Moreover, employees should be given notice of the fact that searches may be conducted. A well-designed employment policy addressing these issues is essential. A sample policy is attached to the end of this chapter, which addresses some of these issues in regard to voicemail and e-mail.

The Federal Electronic Communications Privacy Act

The Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2701 *et seq.*, outlaws the "interception" of electronic communications. Interception is defined under the ECPA to include the aural or other acquisition of the contents of any wire, electronic, or oral communication. It is the term "or other" that applies when dealing with e-mail and other new technologies. Although electronic communications are now covered by the ECPA, the courts have narrowly interpreted the range of protection afforded by the prohibition against interception.

The ECPA clearly gives an employer the right to access an employee's e-mail and voicemail messages if the messages are maintained on a system *provided by the employer*. However, employers may not access messages if the system is provided by an outside entity such as MCI Mail without the authorization of the employee who communicated the message or the intended receiver of the message.

Once the employer has accessed messages, it must be very careful about divulging their contents. The Act prohibits certain unauthorized knowing disclosures. The employer may disclose the message to the addressee or intended recipient or to an agent of that person. The employer may also disclose the contents of the stored messages with the lawful consent of the originator or addressee of the message or the intended recipient of the message.

Thus, one method of limiting potential legal exposure is to conduct only "authorized" searches and retrievals, and to limit the scope of search-and-retrieval efforts to that which is business-related. Similarly, a well-established written policy regarding the employer's ability to search and retrieve voice- and e-mail messages also will assist employers in demonstrating that their conduct is "authorized."

Employers should note that the ECPA also protects against the unauthorized access of electronic communications in electronic storage. E-mail in electronic storage includes e-mail that has been stored for backup protection. By definition, most e-mail exists in electronic storage. Therefore any protection of employee privacy found in the ECPA will generally be based upon the unauthorized access provision.

The Federal Omnibus Control & Safe Streets Act

Title 18 of the United States Code regulates the interception of wire, electronic, and oral communications. The applicable provisions operate as minimum national standards. *United States v. Capra*, 501 F.2d 267, 276 (2d Cir. 1974), *cert. denied*, 420 U.S. 990 (1975). **Section 2510 of Title 18 sets forth relevant definitions and section 2511 outlines prohibited conduct amounting to criminal activity. Prior to 1986, Title 18 pertained only to wire and oral communications, but in 1986, Title 18 was expanded to cover "electronic" communications.

Section 2511 prohibits an individual from intentionally intercepting "any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). *Intercept* is defined as the "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Although the law is highly unsettled, a circuit court of appeals has held that the retrieval of a telephone message from an electronic digital display-type pager did not constitute an "interception" of the transmission. *United States v. Meriwether*, 917 F.2d 955 (6th Cir. 1990). The court reasoned that the transmission over the system had ceased by the time the agent retrieved the information by pushing the digital display button. Accordingly, under *Meriwether*, if the employer merely retrieves information, the employer has not engaged in an interception of information as prohibited by Title 18.

The Consent Exception

Perhaps the most significant exception to the Safe Streets Act is found in 18 U.S.C. § 2511(2)(d), which provides that an employee may either expressly or impliedly consent to an otherwise impermissible monitoring of a communication. Accordingly, employers may avoid liability under the Safe Streets Act by procuring the consent of employees before monitoring communications. Because determining whether there is implied consent is highly fact specific and uncertain, employers should try to obtain express consent in writing.

When determining whether implied consent has been obtained, many courts distinguish between the implied consent to search and retrieve business-related information and personal information. This is especially true if the communication system is available for personal use or if other reasonable alternatives for communicating personal information do not exist. *Watkins v. L.M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983) (rejecting a claim that the employee had impliedly consented to the interception of a personal call after determining that the employee had consented to the company's policy of monitoring business calls but not personal calls). *But see Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392, 396 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979) (finding that implied consent existed after acknowledging that the defendant company had a well-known monitoring policy and prohibition against using monitored phones for personal calls and that the employee had received numerous warnings regarding excessive use of these lines for personal reasons). Whether implied consent exists often depends largely upon how a company's search and retrieval policy is explained and understood. *Watkins*, 704 F.2d at 581. Accordingly, company policy should be carefully tailored so as to reduce employees' expectations of privacy and limit potential exposure.

Employers should be aware that a provision in an e-mail policy that merely suggests that monitoring may be done, such as one that reads: "Company reserves the right to monitor all e-mail communication," may not be sufficient to create implied consent. In *Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992), the employer told his employees that he might be forced to monitor calls if the store's telephone continued to be used for personal calls. Despite the employee's awareness of the threat of monitoring, the court held that there was no implied consent, because the employee was not informed that she was being monitored. *Id*. at 1157. Therefore, mere knowledge of the possibility of monitoring is insufficient. Employers should instead explicitly inform all employees that monitoring will take place.

Business Extension Exception

The Safe Streets Act prohibits interception only through the use of any "electronic, mechanical, or other device." It excludes telephone equipment or components thereof furnished to the user by a provider of wire or electronic communications service in the ordinary course of business and being used by the subscriber in the ordinary course of business. 18 U.S.C. § 2510(5)(a). Thus, monitoring voicemail retrievable systems furnished by a communications service, such as Pacific Bell, and used during the ordinary course of business, may not constitute an "interception" for the purposes of this statute. Although it is unclear whether this exception would apply to a voicemail system, it appears less likely to apply to an e-mail or other system that does not rely on a "telephone or telegraph instrument, equipment or facility, or any component thereof."

To fall within the ambit of this exception, monitoring also must take place within the "ordinary course of business." 18 U.S.C. § 2510(5)(a). *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 740 (4th Cir. 1994); *Briggs v. American Air Filter Co., Inc.*, 630 F.2d 414, 419-20 (5th Cir. 1980); *Campiti v. Walonis*, 611 F.2d 387, 394 (1st Cir. 1979); *United States v. Harpel*, 493 F.2d 346, 349 (10th Cir. 1974). A general policy of monitoring does not by itself render monitoring of any particular call or piece of information as occurring in the ordinary course of business. Rather, every particular monitoring activity must be separately considered to determine whether it occurred in the ordinary course of business. Courts addressing the questions of whether telephoning monitoring or recording of a telephone conversation occurred within the ordinary course of business have differed sharply in standards and criteria employed in their corresponding determinations. Furthermore, little case law exists to provide guidance regarding the applicability of this exception to searches and retrieval of information from voicemail, e-mail, and related message systems.

For this exemption to apply, the employer would have to be classified as a system provider or an agent of a system provider. It is possible that an employer could qualify as a system provider, if the company had its own e-mail system on their own interstate network. For employers who provide their own company e-mail, there are two additional theories to support the conclusion that the ECPA does not affect them. The first theory is available for employers with a system whose messages remain entirely intrastate, and is based on the ECPA's applicability being limited to interstate communications. Thus, such a network would not fall within the definition of "electronic communication service," and is thus outside the protection of the ECPA. However, this theory has not been tested and success under this theory is not clear, particularly when one considers the breadth commonly given to the phrase "affecting interstate commerce" in Commerce Clause cases. The second theory rests upon the ECPA's clear exemption of system providers from its prohibition against access and disclosure of stored electronic communications. The legislative history of the act provides little guidance as to whether Congress intended to exempt private companies who provide their own e-mail system as system providers. The uncertainty of Congress' intent may lead courts to craft a narrow definition of the term "system providers," under which only public, commercial providers such as America Online are covered. Given the potential difficulties inherent in these arguments, an employer is best advised to rely upon the general business use exemption outlined above.

Recent Legislative Activity

Electronic monitoring has received a great deal of recent attention and legislative scrutiny. Last fall, the California Legislature passed Senate Bill 1016, which would have created new privacy rights for employees. The bill made it a misdemeanor for employers to monitor an employee's e-mail without giving prior notification of such monitoring. It also afforded employees the right to access and dispute records collected by their employer through electronic monitoring. After much lobbying on both sides of the issue, Governor Gray Davis vetoed the bill on October 10, 1999, calling it a trap for the unwary but well-meaning employer. Daily Lab. Rep. (BNA), Oct. 15, 1999, at A-4.

State Law & Common Law Privacy Rights

Employers should be aware that state statutes and state common law may also limit the nature and scope of permissible searches. At least one state, California, has a constitutional right to privacy that applies to private employers. In addition, several states have created a statutory right to privacy. (See statutes cited in the Reference Table at the end of Chapter 21 of The 2000 National Employer®.) For example, Massachusetts has enacted the following privacy statute:

> A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages.

Mass. Gen. Laws ch. 214, § 1B (1989).

Some states, such as Alabama, have provisions in their state's constitution mirroring the Fourth Amendment. States that explicitly guarantee a right to privacy in their constitutions are Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington.

In addition to statutory restrictions, courts in almost all state jurisdictions have long recognized various common law causes of action involving the intrusion into the personal privacy of individuals: (1) misappropriation of the name and likeness of another, (2) unreasonable intrusion upon the seclusion of another, (3) unreasonable publicity given another's private life, and (4) publicity that unreasonably places a person in a false light. (For a more extensive discussion of these causes of action, see Chapter 21 of The 2000 National Employer®.) These torts can readily be applied to electronic searches. For example, the tort of unreasonable intrusion upon the seclusion of another may be claimed when an employer engages in an unreasonable or unwarranted search of an employee's voicemail or e-mail. This risk would be increased if the employer has failed to adequately reduce the particular employee's expectation of privacy.

In some states, plaintiffs may bring a common law action for "invasion of privacy." For instance, in one California case, an employee brought a class action lawsuit alleging that the employer invaded the employees' privacy by circumventing their passwords and reading their e-mail messages while fostering an atmosphere that led them to believe their messages were private. The court refused to extend California's right of privacy to employee e-mail, suggesting that such a determination should be left to the legislature. *Flanagan v. Aepson*, Case No. BC-0670-36 (L.A. Sup. Ct. 1990). Recently, another employee brought an invasion-of-privacy claim in Texas state court based on an employer's review of e-mail messages stored on the Plaintiff's computer workstation in a password-protected "personal folder." *McLaren v. Microsoft Corp.*, 1999 Tex. App. LEXIS 4103 (May 28, 1999). The company reviewed the plaintiff's e-mail as part of its investigation of sexual harassment allegations levied against the plaintiff. Finding that the plaintiff could have no reasonable expectation of privacy in e-mail messages stored on the plaintiff's company computer, which was provided to him solely for the performance of his job, a Texas appellate court affirmed the dismissal of the suit. *Id.* at *11. In another example, an employee asserted an invasion of privacy claim based upon an investigation by the employer that consisted primarily of conversations with coemployees. The Alabama Supreme Court held that the employer had the right to reasonably investigate the complaints against the employee, but did note that, even when monitoring is based on a legitimate right, employers should be cautious about intruding into the personal lives of the employee. *Nipper v. Variety Wholesalers, Inc.*, 638 So. 2d 778 (Ala. 1994).

Thus, private employers must consider how state privacy law and common law privacy rights may impact company policies on monitoring searches to ensure that they do not impinge on an employee's state law right to privacy. A complete discussion of the privacy law in each individual state, and its application to searches in the digital workplace is beyond the scope of this chapter.

For more information on state privacy laws and privacy rights provided by state constitutions, see Chapter 21 of The 2000 National Employer®.

Reducing Employees' Expectations Of Privacy

The single most important point for employers to remember regarding privacy in the digital workplace is the need to reduce employees' expectations of privacy in the workplace. Examples abound where employers have successfully defended against privacy claims by taking this simple step. One employer placed a sign about twelve feet above the entry to its building that read "entry into this facility grants permission for a search." A person then walked past that sign and entered onto the property. When that person was leaving, a security guard requested the person to step aside for a body search. The court held that the sign was sufficient to reduce the expectation of privacy of any person entering the premises. Therefore, the court held, the body search was not an impermissible invasion of privacy.

To reduce an employee's expectations of privacy, employers should be open and clear about the company's intentions. An employer should develop Internet and e-mail policies that effectively lower the expectation of privacy in advance, present them to the employees in writing and through training programs including, if possible, actual demonstrations. This will greatly improve an employer's chances of tipping the privacy balance in its favor in future litigation challenging the surveillance or monitoring. The lower the expectation of privacy on the part of the employee, the greater the likelihood that searches and monitoring will be held valid. The bottom line is that the employer should do everything it reasonably can, consistent with its culture and employee morale, to lower the privacy expectations of employees. A sample notice to employees of the type that could be used to help accomplish this task has been included at the end of this chapter.

Conflicting Privacy Policies

In an effort to avoid violating the privacy rights of employees, many employers wisely implement a policy that reduces employee privacy expectations by stating that e-mail communications and computer use are not private and may be monitored by the employer. However, such policies may conflict with other workplace policies that ensure privacy and confidentiality. Imagine this scenario:

> An employer implements a policy that clearly states e-mail and computer use are not private and may be monitored by the employer. The employer has another policy that states employees may confidentially contact the Employee Assistance Program for private counseling sessions. An employee sends an e-mail to the Employee Assistance Program requesting counseling for depression. The employer who monitors employee e-mails reads this e-mail regarding confidential counseling.

Has the employer violated the employee's right to privacy? While one policy stated that e-mails are not private, another expressly gave employees the right to confidentially request counseling. Imagine another scenario:

> An employer implements a policy that clearly states e-mail and computer use are not private and may be monitored by the employer. In addition, the employer has a policy regarding sexual harassment that clearly states all complaints about sexual harassment will be strictly confidential. An employee sends an e-mail to the Human Resources Department complaining about a supervisor's sexually offensive behavior. That supervisor is responsible for monitoring employee e-mails and happens to read the e-mail sent to Human Resources.

Given that the employee was assured that all complaints would remain strictly confidential, has her right to privacy been violated?

To avoid problems like the above-mentioned scenarios, employers should include a disclaimer regarding the nonconfidential nature of e-mail, voicemail and computer communications in any policy that provides assurances of privacy to employees.

Disclosure Of Private Employee Information

Once a company connects its computer network to the Internet, the risk of private employee information being made public increases. As a result, an employer's liability for invasion of privacy claims also increases. Consider the following:

> An employer unfamiliar with the Internet attempts to send an employee's medical records to the Human Resources Department. He hits the wrong keys, however, and sends the records to all e-mail addresses on the company's mailing list.

Although it was unintentional, the employer will likely be held liable for violating the privacy rights of the unfortunate employee. In addition, the employer could be held liable for violating a law such as California's Confidentiality of Medical Information Act, California Civil Code section 56, which prohibits employers from disclosing medical information without employee consent. Imagine another scenario:

> An employer enters the medical records of all employees onto the computer network. He does not protect the information with any encryption technology. An outside computer hacker breaks into the computer system, downloads the files, and posts them on an Internet message board.

Will the employer be held liable for violating the privacy rights of the employees? Does the employer have a duty to protect private information from outside hackers? If so, what is that duty? Must an employer use encryption technology and if so, must the most advanced encryption technology be used? What if an employer cannot afford the most advanced encryption technology?

The answers to these questions are not clear. While these situations are bound to come up, they have not yet reached the courts. Until more answers are available, employers need to be aware that private employee information should be protected and handled carefully. The Internet presents opportunities for such information to be broadcast to millions of people. A company that is connected to the Internet must take extra precautions when transmitting private employee information over the computer network.

Anonymous Message Senders

Privacy advocates extol the virtues of anonymity and claim that if the right to be anonymous in cyberspace is taken away, the entire nature of computer communication will be damaged. While the right to privacy is very important, the anonymity available to users of the Internet creates many problems for employers. Imagine these scenarios:

> Someone is posting defamatory statements about Company X on financial bulletin boards. The statements range from accusations that the company is financially unstable to claims that the president is a thief. The employer believes that a recently demoted employee is responsible for posting the messages, but is not certain because the sender's computer identity is unrecognizable.
>
> Someone is sending harassing e-mails to a female employee but the sender's identity cannot be determined. Recognizing its duty to prevent sexual harassment in the workplace, the employer attempts to find out who is sending the harassing e-mail messages.

In the above scenarios, the employers are powerless to stop the improper behavior unless they are able to determine the identities of the senders of these messages. Can the employers contact the senders' Internet service providers (ISPs) to get information regarding the identities of the senders, or would doing so constitute an invasion of the senders' privacy?

Although the law is still developing in this area, it seems as if employers in certain situations can obtain the actual identity of the sender from the service provider without running afoul of privacy laws. The Electronic Communications Privacy Act, one of the laws governing privacy, does not prohibit employers from contacting the service providers. If the employer is the government, the Electronic Communications Privacy Act does require a subpoena, a warrant, or the consent of the employee before seeking such information from service providers. 18 U.S.C. § 2703(c)(1)(B) and 2707. *See McVeigh v. Cohen*, 996 F. Supp. 59 (D.D.C. 1998) (U.S. government, as employer, improperly obtained the identity of an America Online user without a subpoena, a warrant or consent of the user).

Once a service provider is contacted, will it comply with the request for information and reveal the identity of its customer? It depends on the circumstances. Most service providers have privacy policies that limit the circumstances in which they will disclose information about customers. Many of these policies state that unless served with a subpoena, a warrant or a court order, they will not disclose customer information. A recent case illustrates the situations in which an ISP will provide information about a user's identity.

In that case, the customer exacted revenge on her husband's ex-wife by posing as the ex-wife online and posting messages soliciting sexual encounters. The postings listed the ex-wife's phone number and encouraged people who wanted to engage in sex with her to call the number. After America Online was served with a subpoena from the ex-wife's lawyer, it revealed the identity of the person who sent the messages. The customer then sued America Online for revealing her identity, but the court found that the ISP did not violate any laws when it revealed the customer's identity. *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105 (E.D. Mich. 1998).

So long as an employer is able to meet the requirements of the ISP's privacy policy, that employer will most likely be able to get information from the ISP regarding the identity of the sender of the messages. However, getting the providers to cooperate may not always solve the problem. All an ISP can reveal is the information given to it. If that information was inaccurate or false, the employer will be unable to uncover the identity of the sender of a particular message.

HEALTH & SAFETY ISSUES

Coverage Of Home Office Workers

On November 15, 1999, the Labor Department's Occupational Safety and Health Administration (OSHA) issued a letter of interpretation to a credit service company in Texas which had requested guidance on permitting some employees to perform work at home. The letter, which caused an immediate furor, implied that OSHA now considered federal workplace safety rules to apply to millions of telecommuters.

In the face of mounting criticism, on January 5, 2000, the Labor Department Secretary Alexis Herman issued a formal statement withdrawing the advisory letter. <http://www.osha.gov/media/oshnews/jan00/statement-20000105.html>. In her January 5 statement, Secretary Herman called for a "national dialogue" on the issue and declared her intention to begin this dialogue by hosting a future meeting of business and labor leaders. Three weeks later during congressional hearings on the issue, Assistant Secretary for OSHA, Charles Jeffress, stated his regret over the "confusion" caused by the advisory letter, emphasizing that OSHA "ha[s] not inspected home offices; and we have no intention of inspecting home offices." Brian Krebs, *Labor Dept. Withdraws Letter, Faces Criticism*, Newsbytes, Jan. 28, 2000. Thereafter, on February 25, 2000, OSHA issued a new compliance directive, declaring that OSHA would not seek to hold employers liable for an employee's home office, but would follow-up on complaints involving potentially hazardous factory work being performed in homes. <hhtp://www.osha.gov/media/oshnews/feb00/national-20000255.html>

The permanence of this retreat will likely depend on the outcome of 2000 Presidential election. Under a Gore administration, an activist Department of Labor can be expected to revisit the issue.

OSHA's Sweeping Ergonomics Proposal

The increased use of computers will undoubtedly subject employers to an ever-increasing array of ergonomic-related claims, especially ones by employees who are just beginning to use video display terminals (VDTs) and keyboards. Employers can expect claims of cumulative trauma disorder (CTD), vision ailments, and fatigue. The scientific underpinnings of ergonomic regulation are uncertain and continually developing as new research becomes available. Unfortunately, the emphasis on quick development of the information superhighway may lead to premature development of regulations in this complex area.

After years of intense controversy, Congressional action and vigorous debate among regulatory officials, unions, occupational health experts and employers, Fed-OSHA recently published a proposed rule to establish a general industry standard on workplace ergonomics programs. The rulemaking initiative, which OSHA Administrator Charles Jeffress vows to complete in 2000 (before the Clinton Administration leaves office), long has been a principal regulatory priority of organized labor, and has been opposed just as vigorously by most employers and industry groups.

Even prior to the development of this new rule, OSHA has been investigating working conditions that appear to trigger "musculoskeletal disorders" for many years, and has cited employers (often through "egregious," sizeable penalties) under the "general duty clause" of the Occupational Safety and Health Act (OSH Act) found at section 5 (a)(1) of that statute. Although OSHA has had difficulty in successfully prosecuting contested ergonomics cases, it entered into a series of widely publicized settlement agreements, some of which covered all of a cited corporation's facilities, rather than the single site subject to inspection and citation. These agreements have imposed substantial financial penalties, and have required adoption of detailed workplace ergonomics programs.

Intense controversy has surrounded the development of ergonomics rules. Employers often argue that not enough is known about the role of work and other identified "risk factors" in the development of targeted health problems to warrant regulation. They also note that such regulatory requirements will impose very substantial costs without any clear or demonstrable benefit (due to the absence of clear and predictable "cause-and-effect" relationships between stressors and individual injuries). Unions, some academics and some regulators feel that adequate science and real-world experience demonstrate the clear connection between the identified stressors and employee injury. Congress, which had previously blocked regulatory action by OSHA in this area, has appropriated funds for a National Academy of Sciences study of the existing scientific literature on these points. A House-passed bill, the "Workplace Preservation Act," would block OSHA's final action on this rulemaking until that study is complete.

Basic Coverage Provisions

The regulation proposed by OSHA would apply automatically to employers with employees who work in "manufacturing" or "manual handling" jobs, as those terms are defined by the rule. In addition, the regulation would apply to other employers whose employees report one musculoskeletal disorder (MSD) after the rule's effective date, where the physical activities and conditions on the job are

"reasonably likely to cause or contribute to" the condition, and where those activities and conditions are either a core element of the job, or require a significant amount of the employee's worktime. While the rule incorporates a job-based "trigger" (meaning that it only applies to the jobs in which such conditions exist, rather than an entire company or work site), the broad definitions are expected to entail coverage for employers in a wide range of industries. (Agricultural, construction, and maritime operations are excluded from this proposal.)

OSHA proposes to define MSDs as injuries and disorders of the muscles, nerves, tendons, ligaments, joints, cartilage and spinal discs. Examples of MSDs given in the proposed standard include carpal tunnel syndrome, rotator cuff syndrome, De Quervain's disease, trigger finger, tarsal tunnel syndrome, sciatica, epicondylitis, tendinitis, Raynaud's phenomenon, carpet layers' knee, herniated spinal disc, and low back pain. However, MSDs would not include injuries caused by slips, trips, falls, or other similar accidents.

Program Elements

Employers whose employees work in manufacturing or manual handling jobs will be required to implement two elements of the ergonomics program ("Management Leadership and Employee Participation," and "Hazard Information and Reporting"), even if no MSD has occurred in those jobs. In other employment positions, employers must comply with a series of program elements if a covered MSD is reported or if the employer is aware of an ergonomic hazard, unless the MSD hazards are eliminated using a "Quick Fix" option, discussed below.

Employers would be able to continue their existing ergonomics programs if they can show that those programs satisfy the basic requirements of each program element in the proposed standard. Employers would be required to be in compliance with the recordkeeping requirements of the proposed standard and would need to show that they have implemented and evaluated an effective program and appropriate control measures before the effective date of the proposed standard. These employers would have to perform a program evaluation that shows their ergonomics programs are functioning properly and are in compliance with hazard controls described in the proposed standard.

Basic Programs

The proposed standard would require employers with manual handling or manufacturing production jobs to assign and communicate responsibilities for setting up and managing the ergonomics program so managers, supervisors, and employees know what is expected of them and how they will be held accountable for meeting those responsibilities. These assigned employees must be given the authority, "resources," information, and training necessary to meet their responsibilities. Employers would also be required to provide employees (and their designated representatives) with ways to report "MSD signs" and "MSD symptom"; get responses to reports, and be involved in developing, implementing, and evaluating each element of the program. Employers would be prohibited from policies or practices that discourage employee participation in the program, or discourage reporting MSDs signs or symptoms.

The second element of a basic program would require employers to periodically provide information to employees explaining the contents of the OSHA standard, ergonomic risk factors, signs and symptoms of MSDs and the importance of early reporting of MSDs. The employer would also be required to evaluate employee reports of MSD signs and symptoms to determine whether a covered MSD has occurred.

The "Quick Fix" Option

The "Quick Fix" alternative described in the proposed standard is intended to address situations that can be remedied immediately. Employers would be required to provide prompt care for injured employees and to work with employees to implement corrective measures within ninety days of an MSD. The employer would then be required to evaluate the effectiveness of their corrective measures within thirty days after implementation of those measures. The evaluation and implementation of corrective measures must be documented and the employer must implement a full ergonomics program if the remedies fail or if another MSD of the same type occurs in the same job within thirty-six months.

Full Program Elements

Employers with covered MSDs as described in the proposed standard would be required to implement additional elements of a full ergonomics program, including job hazard analysis, control and employee training. These would include analyzing problem work tasks for ergonomic risk factors and working with employees to minimize risks using engineering, administrative and/or work practice controls. Use of personal protective equipment (PPE) by employers is primarily intended to supplement these other controls; PPE can be utilized by itself solely in circumstances in which other controls are not feasible. The full program must also include a

mechanism to track progress and to identify and evaluate MSD hazards whenever new or modified tasks are introduced.

Effective Dates Of Key Provisions

The Ergonomics Program Standard would become effective sixty days after publication of the final rule. Individual provisions would be phased in as follows. One year after the effective date, management leadership, employee participation, hazard information, and reporting must be in place. Two years after the effective date, job hazard analysis, training and interim controls must be completed. Three years after the effective date, employers must have permanent controls and program evaluations in place.

Outlook For Final Agency Action

OSHA's leadership has committed the agency to move with the regulatory equivalent of the "speed of light" on the ergonomics standard. They have a goal of going from a proposed standard to final agency action in one year. Most standards take the agency several years (or longer) to finalize, even from the point of the rule's formal proposal. This emphasis on speedy action is derived from the perception of OSHA's leadership that this is a critical area of workplace safety and health that must be addressed, the push that comes from the Administration's supporters in organized labor, and concerns about the priorities of new agency leaders after the 2000 Presidential election. Given the high stakes associated with this regulatory proposal, the policy debate and the political battle that will unfold over the coming months will be of great interest to all employers.

For more information about Fed-OSHA regulations, see Chapter 32 of The 2000 National Employer®.

State OSHA Ergonomics Regulations

To date, only one state OSHA agency has developed detailed ergonomic regulations. On April 17, 1997, the California Occupational Safety and Health Standards Board (the Standards Board) adopted the nation's first regulation governing ergonomics in the workplace. The California Office of Administrative Law (OAL) approved the regulation on June 3, 1997, and it became effective on July 3, 1997. This highly controversial regulation standard may apply to *any* employer in California, and applies to *every* industry. Employers can anticipate that this new regulation will result in a substantial number of employee complaints concerning ergonomics, an increase in workers' compensation claims asserting injuries/illnesses associated with ergonomics, and substantial enforcement activity by the Division of Occupational Safety and Health (the Division), the enforcement arm of Cal-OSHA. It is also likely to generate similar or even more rigorous regulation of ergonomics on the federal level and/or in other states.

Internet Health & Safety Information

Fed-OSHA has a Web site at <www.osha.gov> that provides helpful information for employers regarding an employer's duty to maintain a safe workplace.

While the Web site offers much information that can help an employer, it also offers information that can be used to harm an employer. Anyone with Internet access can visit the OSHA Web site and quickly and easily access a record of a particular employer's OSHA compliance history. An employee, a potential client, a union representative or an OSHA compliance officer can obtain a listing and a detailed description of each inspection since 1972 and the citations issued for each inspection. While this information has always been available to the public under the Freedom of Information Act, before the creation of the Web site, one had to fill out a form and write a letter to obtain such information. Today, all one has to do is log onto the Internet and the information is available within seconds. This new easy access to an employer's OSHA information has many implications for an employer.

Even though the Web site is an official OSHA site run by the government, it can provide an inaccurate impression of a company's OSHA compliance. First, the site is not always accurate. Sometimes, the information regarding a particular citation is incorrect or the site may show that an employer received a citation when in fact, none was ever given.

In addition, the information on the Web site is not always current. The entries can run up to six months behind. Thus, if an employer received a citation but later got the citation vacated, it may take up to six months for this information to appear on the site. In the meantime, anyone who uses the Web site to look up that employer's compliance history will see that the company was cited, but will not see that the citation was vacated. Also, when a citation is vacated, the citation is not removed from the site. The citation remains, but a notation is made next to it that the citation was vacated.

Another opportunity for an inaccurate impression of a company's OSHA compliance can be illustrated by the following example:

An angry employee wants to get dirt on his employer. He visits the Web site to see how many times his

> employer received OSHA citations. His company's name is Northwest Roofing Co. He types in "Northwest" and over a hundred inspections and citations appear. He immediately tells his fellow employees about the numerous citations. What he failed to notice in his rush to find dirt on his employer was that the Web site search he typed in brought up information, not only about Northwest Roofing Co., but also about Northwest Plastics, Northwest Shoe Repair, Northwest Machine Co., etc. Thus, all of the information he thought applied to his employer actually applies to several different employers.

The fact that the Web site can provide an inaccurate picture of an employer's OSHA compliance is troubling. The information on the OSHA Web site, whether it is correct or not, can be used against an employer. For example, unions can use the information to encourage employees to unionize. A string of health and safety violations, regardless of whether the violations actually occurred or are simply mistakes on the OSHA Web site, can convince employees that their employer does not care about workplace safety and can make joining a union seem like the right thing to do.

Electromagnetic Fields & Radiation

Recent news reports have voiced concern over the potentially damaging health effects of electromagnetic fields (EMFs) and radiation from computer terminals. State and federal regulatory agencies have begun to respond to public concern about these issues. To date, however, there seems to be little scientific evidence to suggest that a hazard of this nature exists.

However, the fear of EMF exposure and/or radiation exposure may be a compensable injury under workers' compensation. Employers should keep abreast of scientific evidence on the potential health effects of EMFs, and related subjects, and be prepared to educate their employees about scientific studies concerning this issue.

VIRTUAL WORKERS AND TEAMS ON THE INTERNET

The digital workplace revolution is most evident in the increased reliance on telecommuting and other flexible work arrangements. A survey by the International Telework Association found that telecommuting among U.S. workers has risen thirty percent since 1995. One study suggests that the number of telecommuting employees could reach fifteen million by 2002. In 1997, it was estimated that eleven million individuals telecommuted, and that telecommuting has grown thirty percent since 1997. Furthermore, employers surveyed in 1998 believe that by the year 2001 telecommuting will have increased by eighty-five percent. One commentator noted, "Work is now in the electronic network, not in the office." John Sharp, *Notes on "Going Virtual" by Ray Grenier & George Metes*, Oct. 1996 <http://www.tfriend.com/cop/n-govirt.html>. As technology evolves, the office is becoming less and less important. Technology allows workers to communicate and work together regardless of where they are. No longer do employees have to meet in the office to discuss business. Today, employees in different cities and even different countries can work together in cyberspace, just as effectively and efficiently as if they were sitting side by side in an office.

While virtual workers and virtual teams are beginning to become more common, they still present some novel legal issues and dilemmas for employers who utilize them. Before jumping on the virtual bandwagon, an employer should familiarize itself with the issues implicated in hiring virtual workers and assembling virtual teams. Otherwise, virtual workers could create very real problems for employers.

Without face-to-face interaction, it is more difficult to build the rapport that is necessary for a team to function effectively. Employers need to put in extra effort to ensure that a team culture is cultivated. In addition, with virtual team members from countries around the globe working together, the chance for misunderstandings and cultural insensitivity increases. Employers may find it helpful to train virtual team members on how to work effectively with members from different countries and how to respect the different cultures represented on the virtual team.

Research has shown that people are not likely to collaborate with each other if they work more than fifty feet apart. This has come to be known as the "fifty-foot rule." Kevin Pierce, *Review by Kevin Pierce* (visited Mar. 30, 1999) <http://www.netage.com/vt/virtualteams/reviews/pierce.htm>. Technology has basically abolished the fifty-foot rule. Employers are increasingly relying on virtual teams to solve problems. Virtual teams free companies from the boundaries of time and space and allow them to utilize the skills of employees from around the world to solve common issues or problems. Employers no longer have to staff people on a project simply because they are the employees who happen to be in the office. Now, an employer can staff the most knowledgeable people on a project, regardless of where they might be at the time.

Amid increased competition for workers, telecommuting has also emerged as a recruiting tool. This strategy is particularly common among high-tech firms. Over eighty-two percent of all high-tech firms now permit some form of telecommuting. In testimony before Congress, Charles Grantham, author of *The Digital Workplace* made the following statement regarding the increased use of

telecommuting in the U.S. workforce:

> This trend [toward increasing use of telecommuters] will continue as technology infrastructure becomes more ubiquitous and cost pressures continue the corporate downsizing trend in the U.S. U.S. industrial competitiveness can be improved by significantly expanding the use of these work options. Increases in productivity and creativity that we have documented can be sustained over long periods of time. U.S. workers can begin to import work from other countries that they are uniquely qualified to do, such as software design, information brokering and other highly symbolic analytic work.

Telecommuting is an attractive option for employees because it often provides increased flexibility and greater control over the employees' work environment. Benefits to employers include savings on office overhead, lower employee absenteeism, increased productivity, improved employee morale, and higher employee retention. George M. Piskurich, *Making Telecommuting Work*, Training & Dev., Feb. 1996. Telecommuting also reduces traffic congestion, air pollution, and energy consumption. Employees avoid the costs and stresses of commuting, incur reduced expenses for work attire, and can more easily make child care arrangements.

The benefits associated with a digital workplace, such as an increase in productivity and information flow, cannot be disputed. The General Services Administration estimates that telecommuting employees are twenty percent more productive than their in-office counterparts. Other benefits include savings on real estate costs–in 1994, thirty-five thousand AT&T managers telecommuted, resulting in an eighty-million-dollar reduction in real estate costs. As companies rush to create a digital workplace to improve their productivity, however, they must consider the full impact that new technology will have on their workforce. Many companies have chosen to ignore the full impact of the technology and continue to operate with a "business as usual" attitude. By focusing attention on potential legal problems now, employers will avoid having to focus on them later in costly litigation.

The Americans With Disabilities Act

The Internet has had a significant impact on the area of disability in the workplace. A new disability known as Internet Addictive Disorder is an illness caused by the Internet and is an issue that will likely confront employers in the near future. In addition, the Internet has had an impact on what reasonable accommodations an employer may be required to provide for disabled employees.

Presence As An Essential Job Function

The Internet has made telecommuting easier than ever and has virtually done away with the need to work in an office. The proliferation of companies that no longer have physical headquarters but instead rely on virtual offices proves that the traditional office is becoming less necessary. With Internet access, an employee at home can perform all of the functions an office worker performs and can work just as effectively as someone in an office. Meetings and all other necessary communication can take place over the Internet and research on just about anything can be performed over the Internet. Supplies can be ordered online and delivered right to the telecommuter's door.

For those employees who cannot work at the employer's place of business due to a disability, telecommuting is sometimes an attractive solution. The question, then, is whether an employer is required under the Americans with Disabilities Act (ADA) to permit a disabled employee to telecommute as a reasonable accommodation. The ADA requires covered employers to make reasonable accommodations for otherwise qualified employees with disabilities. 42 U.S.C. § 12112(b)(5). When employers refuse to make reasonable accommodations for qualified disabled employees, they can be sued for discrimination. Telecommuting is an attractive solution for many employees who cannot work at the employer's place of business due to a disability. However, the federal courts are currently split on the issue of whether an employer is required under the ADA to permit a disabled employee to telecommute as a reasonable accommodation.

In one of the first cases to consider telecommuting as a reasonable accommodation, a federal court held that employers are not generally required to accommodate a disability by allowing a disabled worker to work at home. *Vande Zande v. Wisconsin*, 44 F.3d 538 (7th Cir. 1995). Vande Zande claimed a violation of the ADA and the Rehabilitation Act for her employer's failure to reasonably accommodate her disability when her employer refused to install a desktop computer and laser printer in her home as an accommodation and refused to allow her to work at home for a full workweek. The court rejected her claim and ruled that the employer had no obligation under the ADA to accommodate Vande Zande by allowing her to work at home and had no duty to install a desktop computer and a laser printer in her home. The employer's decision to allow Vande Zande to work at home for a limited number of hours a week, requiring her to use sick time for the remainder of the hours and limiting her to a laptop computer, was held to be more than reasonable as an accommodation. In support of its ruling, the court stated the following:

> Most jobs in organizations, public or private, involve team work under supervision rather than solitary

> unsupervised work, and team work under supervision generally cannot be performed at home without a substantial reduction in the quality of the employee's performance.

Id. at 544.

Is presence an essential function of the job? Those courts that believe that it is focus on the disruption caused to a company's operations when an employee is not reliably present. Under this line of reasoning, if physical presence at work is an essential function of employment, then telecommuting is not a reasonable accommodation. In *Vande Zande*, the court held that most jobs cannot be performed from home. In particular, the *Vande Zande* court noted that, because most jobs require teamwork, they cannot be performed at home without a substantial reduction in productivity. *Id.* at 544. Similarly, in *Whillock v. Delta Air Lines, Inc.*, 926 F. Supp. 1555 (N.D. Ga. 1995), *aff'd mem.*, 86 F.3d 1171 (11th Cir. 1996), the court held that the plaintiff's request to work at home was unreasonable as a matter of law because the plaintiff could not adequately perform her duties as a reservation sales agent from home. The *Whillock* court relied on three facts in making this conclusion. First, as the reservations agents have access to classified airline information, this information cannot be used off premises without endangering security of the information. Second, agents work in a highly supervised environment where on-the-job training is ongoing and essential. Finally, providing Whillock with her own computer would be disproportionately expensive, as compared with the cost of sharing a terminal with other agents on the site. *Id.* at 1564. In yet another case, a court followed the same reasoning and found telecommuting to be an inappropriate accommodation because an essential function of the plaintiff's job was attending meetings and collaborating face-to-face with colleagues. *Misek-Falkoff v. IBM Corp.*, 854 F. Supp. 215, 226-27 (S.D.N.Y. 1994), *aff'd mem.*, 60 F.3d 811 (2d Cir. 1995).

Vande Zande presumed that telecommuting is not a reasonable accommodation. This view is generally still followed in Illinois and the states within the Seventh Circuit. *Leahr v. Metropolitan Pier & Exposition Auth.*, 1997 U.S. Dist. LEXIS 10601 (N.D. Ill. July 17, 1997). Other courts, however, are recognizing that the *Vande Zande* assumptions no longer hold true. *Hernandez v. City of Hartford*, 959 F. Supp. 125 (D. Conn. 1997). The *Vande Zande* court presumed that most jobs cannot be performed at home without substantial reductions in productivity. However, research shows that telecommuters may be *more* productive than their in-office counterparts. The *Vande Zande* court also assumed that telecommuting is an ineffective accommodation for jobs that have frequent and inflexible deadlines, but e-mail and fax machines now eliminate these dilemmas. Furthermore, if the problem is a need for collaboration, telephone or electronic conferencing now enable a telecommuter to share ideas with colleagues. In one case, a Washington, D.C., federal court held that employers must consider work at home as a potential form of accommodation under the Rehabilitation Act. *Carr v. Reno*, 23 F.3d 525, 530 (D.C. Cir. 1994); *see also Anzalone v. Allstate Ins. Co.*, 1995 U.S. Dist. LEXIS 588 (E.D. La., Jan. 15, 1995) (employer has a duty to consider work at home as an accommodation under the ADA); *Langon v. Department of Health and Human Servs.*, 959 F.2d 1053, 1060-61 (D.C. Cir. 1992). In *Anzalone*, a court denied summary judgment for the employer, and noted that there was no evidence that the plaintiff's productivity declined when he worked from home. Furthermore, the court noted that the employer allowed other claims adjusters to work from home, thus undermining its contention that the plaintiff's job required presence at the office. California courts in particular appear most likely to find that allowing an employee to work at home *is* a reasonable accommodation. *See, e.g.*, *Norris v. Allied-Sysco Food Servs., Inc.*, 948 F. Supp. 1418, 1432 (N.D. Cal. 1996); *Sargent v. Litton Sys., Inc.*, 841 F. Supp. 956, 962 (N.D. Cal. 1994).

The particular facts of *Langon* are illustrative of the new trend in those courts that are finding that telecommuting *is* a reasonable accommodation. 959 F.2d 1053 (D.C. Cir. 1992). On the advice of her physician, Langon, who suffered from multiple sclerosis, asked the Department of Health and Human Services (HHS) for permission to work from home. HHS denied her request, contending that Langon's job as a computer programmer required her physical presence in the workplace. Eventually, HHS terminated her for unsatisfactory performance. Langon filed suit in federal district court under the Rehabilitation Act, which prohibits disability discrimination by recipients of federal funds. Langon argued that the Rehabilitation Act required HHS to allow her to work from home as a reasonable accommodation for her multiple sclerosis. The district court disagreed, but the D.C. Circuit Court of Appeals held that she had offered sufficient proof that working at home was a reasonable accommodation under The Rehabilitation Act. As both the Rehabilitation Act and the ADA require an employer to consider restructuring an employee's job as an accommodation, many courts are starting to view "work in the home" as a natural evolution and reasonable accommodation. As a federal court in California stated, "With faxes and car phones and home offices, it is no longer the case that an employee must always be physically on site in order to perform her job." *Sargent v. Litton Sys., Inc.*, 841 F. Supp. 956, 962 (N.D. Cal. 1994).

Employers must also consider whether state discrimination law will place a duty on employers to consider work at home as an accommodation. For instance, the *Sargent* court held that under state discrimination law, California Government Code section 12940, an employer has an obligation to consider work at home as an accommodation. *Id.* at 961-62.

Another potential discrimination problem that arises under the ADA is not as obvious. The advent and increased use of telecommuting will allow employers to better accommodate the needs of disabled persons who cannot function in a workplace. However, disabled

groups argue that employers will use this technology to isolate them and to hide them from society. The groups charge that employers will go beyond accommodation and use technology to make them invisible to society. The groups fear that employers will place disabled people in telecommuting centers or at home because of the way they look or the way they act while in the work environment. In this instance, the groups argue that the whole purpose behind the ADA mainstreaming disabled persons into the workforce will be defeated.

Internet Misuse Caused By Mental Illness

Whether an employer has twenty employees or two thousand, every employer will likely encounter at least one employee who misuses the Internet. What if an employee is caught for downloading pornographic images from the Internet, but claims his misuse of the Internet is the result of a mental illness? Can an employer discipline the employee? Does the employer have to make a reasonable accommodation for the employee? What would that reasonable accommodation be?

United States v. McBroom, 124 F.3d 533 (3d Cir. 1997), illustrates how Internet use can be a symptom of a mental disability. Although the case did not occur in an employment context, it illustrates an issue that employers may very well have to deal with in the future. Mr. McBroom, a lawyer who was sexually abused as a child, downloaded child pornography from the Internet and was convicted of possessing child pornography in violation of 18 U.S.C. § 2252(a)(4). He claimed he suffered from a decreased mental capacity and should thus have his sentence reduced. According to McBroom, due to his sexual abuse as a child, he was obsessed with pornography and unable to stop himself from downloading it from the Internet. The appeals court held that the fact that McBroom could be suffering from a mental disorder that prevented him from controlling his behavior should have been considered when he was sentenced. Accordingly, the appeals court ordered the lower court to reconsider the sentence in light of the possibility that McBroom was suffering from a mental illness.

Employers may be confronted with someone like McBroom who claims he or she could not control his or her misuse of the Internet at work and that the misuse is a symptom of a mental disorder. In situations where the health and safety of workers is threatened, the employer's right to terminate the employee is clear. However, the employer's rights in other situations are not as clear. If an employer is faced with a situation similar to the one in the *McBroom* case, legal counsel should be consulted before any termination or discipline decisions are made.

Internet Addiction

Consider the following scenarios:

> A mother neglects her children and spends up to twelve hours a day on the Internet. She is arrested for child endangerment.
>
> A college student drops out of sight and cannot be found by his family or friends. Campus police finally locate him in the university computer lab. He had been there for seven days and had run up four hundred dollars in computer charges.
>
> A man is terminated from his job because he spends the majority of working hours on the Internet.

Situations like the ones above are becoming more common and are the result of a new psychological disorder involving an addiction to the Internet. The disorder has been referred to as "Internetomania," "Computer Addiction," "Internet Addictive Disorder," and "Cyber-addiction." Psychiatrists stress that the disorder is as real as any other addiction and must be taken seriously.

Those who suffer from Internet addiction are unable to control their Internet use. People with the addiction can experience physical and psychological symptoms. The psychological symptoms include: having a sense of well-being or euphoria while at the computer;

inability to stop using the computer; craving more and more time at the computer; neglect of family and friends; lying to employers and family about computer activities; and problems with school or job. The physical symptoms include: carpal tunnel syndrome; dry eyes; migraine headaches; backaches; sleep disturbances and eating irregularities. Maressa Hecht Orzack, Ph.D., *Computer Addiction Services* (visited on Mar. 20, 1999) <http://www.computeraddiction.com/>.

As more people become aware of this disorder, employers may be faced with ADA claims from employees with Internet addiction. Whether this disorder will be considered a disability that is covered by the ADA remains to be seen. If it is considered to be a disability, employers will be required to provide reasonable accommodations for those who are addicted to the Internet. Employers need to be aware that Internet addiction is a real problem and must educate human resource managers on how to spot the signs of Internet addiction among employees.

Working In Multiple Jurisdictions

Once an employer ceases to be limited by space, he or she can employ workers from all over the world. However, having virtual teams made up of workers in different states and possibly even different countries creates complicated jurisdictional issues. In some instances, information lawfully released in one state may not be lawfully received in another state. Similarly, monitoring an employee may be lawful when done in the home office but unlawful in the out-of-state satellite office where the employee works. Many states have different and/or unsettled laws regarding privacy, confidentiality, monitoring, and surveillance, etc. Thus, employers must know an ever-increasing number of different state employment and labor laws. Furthermore, employees and/or their attorneys may engage in forum shopping by carefully studying both the law of the state in which the employee is found, and the law of each state in which the employer is found, and make a determination as to where a lawsuit may be most favorably received. Some of these concerns can be addressed in a carefully worded employment contract, but the potential for jurisdictional disputes and conflict-of-law issues remain quite great.

Employers who send information between countries face the same problems. Employers must be cognizant of the other country's respective labor and employment laws, especially that country's laws regarding privacy. The American-based employer cannot assume that all countries view privacy and other employment law issues in the same manner as in America. This is indeed a dangerous assumption.

Generally, individuals and entities are subject to the laws of their states of residence, and are subject to being sued there. For natural persons, one is a resident of the state in which one lives and works. Business entities are residents of the state in which they are organized, and also of every state in which they are engaged in continuous and systematic activity. A corporation is also likely to be a resident of every state where its employees, including telecommuters, live and regularly work. Residents can be sued in courts in their states of residence on any type of claim. The claim does not need to have any relation to the state. Thus, for example, an Indiana corporation with telecommuters in California and employees who reside in Florida could possibly be sued in Indiana, California, or Florida.

For example, if an employer regularly communicates with a virtual worker in a different state, those communications may establish sufficient contacts with that state to support personal jurisdiction over the out-of-state employer. One California court found that sending e-mail messages over the Internet may establish sufficient minimum contacts to support personal jurisdiction over an out-of-state defendant. *Hall v. LaRonde*, 56 Cal. App. 4th 1342 (1997). In contrast, however, a federal court in California found that sending e-mail messages to individuals in another state is not sufficient to support personal jurisdiction over an out-of-state defendant. *Expert Pages v. Buckalew*, 1997 U.S. Dist. LEXIS 12205 (N.D. Cal. Aug. 6, 1997).

Traditionally, the employment and labor laws of the state in which the employee actually works have governed the working relationship. This may be changing, however, in part due to technologies that now permit an employee to work from a home office hundreds, or even thousands, of miles from the employer's place of business. Increasingly, employers are able to hire employees who live and perform their work in a different state, or even in another country. As a result, courts and employers must struggle with the question of which state's laws to apply to the employment relationship.

One might think that Maryland law would govern a contract between a Maryland software company and an employee living and working in Maryland, especially when the contract specified that Maryland law would apply. As one Maryland software company recently learned, however, that very contract could be invalidated under California law. In *Application Group, Inc. v. Hunter Group, Inc.*, 61 Cal. App. 4th 881 (1998), a California appellate court ruled that an employment contract between a Maryland resident and a Maryland corporation, which stated that Maryland law should apply, was not binding under California law. The Hunter Group employed computer consultants, most of whom live and work outside California. All of the non-California employees had employment contracts with The Hunter Group that included covenants not to compete, an agreement that prevented them from working

with any of Hunter's competitors, including California competitors, for up to one year from termination unless the employee was laid off for economic reasons. One of Hunter's employees, who lived and worked in Maryland, signed an employment contract that included a covenant not to compete. When she resigned from Hunter to go work for The Application Group (AGI) (one of Hunter's direct competitors), Hunter sued the employee in a Maryland court for breach of the covenant not to compete. While the Maryland lawsuit was still proceeding, AGI sued Hunter in a California court for a ruling that would have the effect of finding that the covenant not to compete was unenforceable against an employee working for AGI. Strict covenants not to compete are not generally binding in California, and AGI argued that it could not be bound by such a provision because AGI managed all of its employees from California and treated them all as California employees. A California appeals court agreed and decided to apply California's law against noncompete agreements rather than Maryland law, without regard for whether the employees were, at the time the contracts had been made, residents of or working in California. The California appellate court ruled that California public policy prohibiting noncompete agreements prevented Hunter from enforcing its noncompetition agreement against an employee working for AGI, because AGI's employee relationships were governed by California law.

Proficiency Tests

Employers who use the Internet to administer proficiency tests, must make certain the tests are not discriminatory. The use of any employment test is unlawful if the test is found to have an adverse impact on groups protected by Title VII. Employers also must make certain the tests do not discriminate against disabled applicants who may not be able to take tests over the Internet. In addition to making sure the tests are not discriminatory, all preemployment tests should be validated in accordance with the EEOC's Uniform Guidelines. To "validate" a preemployment test means to ensure that it accurately predicts successful job performance. (For a more extensive discussion on preemployment testing, see Chapter 21 of The 2000 National Employer®.)

Workers' Compensation

The issue of employees working at remote locations and at home through telecommuting raises an entire host of questions under the workers' compensation remedial scheme. For example, as in most states, workers' compensation in California is provided for injury or death to an employee "arising out of and in the course of employment." Cal. Lab. Code § 3600. Particularly for employees working in the home, it may be very difficult to determine when these preconditions for workers' compensation exist. The issues of causation and proof will also become increasingly complex. As an example, if an employee trips while walking down a staircase at home and the employee's "office" is at home, was the employee acting in the course of employment while traveling down the stairs?

Work in a home environment also raises an interesting issue regarding potential stress claims. On first impression, one would assume that an employee working out of his or her home will be less likely to file stress claims. On the other hand, the geographic isolation of that employee combined with the fact that the employee in working out of his or her home never really leaves his or her place of employment, may result in additional stress claims.

There are other hidden costs for employers who use telecommuters. For instance, what happens when a telecommuter gets up from his or her home workstation to get a cup of coffee, and then slips and falls in the kitchen. Is the employee covered by the employer's workers' compensation insurance? And what about the telecommuter's child who cuts herself on the scissors sitting on daddy's desk–is the employer liable? Is the employer liable for injuries to guests who come to visit the telecommuter's "office" during working hours? Traditionally, the employer's workers' compensation carrier does not cover accidents that occur off the employer's premises. However, when an employee performs a specific task at home at the employer's request, the employee is covered by workers' compensation. Additionally, an employee who is expected to operate out of his or her own home is covered if he or she is injured while in the course of employment. For example, a sales representative who worked exclusively out of his home suffered a heart attack while shoveling snow so that he could get his car out to call on a customer; he was covered by workers' compensation. *Tovish v. Gerber Elecs.*, 229 Conn. 587 (1994).

And what about accidents between the telecommuter's home and the employer's place of business? Normally, an employee is not covered for an injury that occurred while the employee was on his or her way to work. However, there are exceptions to this rule, particularly when the employee has a secondary work site at home. In that case, an injury occurring on the way between work and the secondary (home) work site is covered, as travel between work sites is considered compensable. The question then arises–when is the home a "secondary work site," so that travel between the home and office qualifies as travel between work sites? Generally, courts consider the regularity of the work done at home, whether working at home is more than just a convenience for the employee, and whether there is business equipment in the home. The first two factors are the most important. Some companies have had trouble getting workers' compensation insurance for their at-home workers because insurers consider it an opportunity for fraud.

Independent Contractor Status

The digital workplace has changed the way many jobs are performed and in so doing, has blurred the line between independent contractors and employees. Federal and state laws that protect workers and regulate the relationship between a business and a worker generally apply only to employees, not to independent contractors. Also, employers normally do not maintain benefits for independent contractors. Currently, confusion exists as to whether the virtual worker is an employee or an independent contractor. Increasingly, these workers are being treated as "employees," despite the fact that they have never appeared at the office or the plant and are subject to a minimal amount of control and supervision from the employer. Confusion about employment status can be very costly for employers. To avoid this confusion, employers should make certain to determine the status of the worker performing the assignment and clearly set forth whether the worker is an employee or an independent contractor.

In determining independent contractor status, the most important factor is whether an employer has the right to control the method and manner used to achieve the results desired. Courts also rely upon the factors comprising the "economic-reality test" in determining independent contractor status. Under the economic-reality test, the court looks to the alleged employee's opportunity for profit or loss depending on his or her managerial skill; the employee's investment in equipment or materials; whether the services rendered require a special skill; the degree of permanence of the working relationship; whether the service rendered is an integral part of the alleged employer's business; and whether the worker's income depends on the alleged employer. (For a more extensive discussion of independent contractor status and current federal enforcement, see Chapter 28 of The 2000 National Employer®.)

It is quite easy to see that the changing nature of the employment relationship in light of the digital workplace will impact the independent contractor analysis. An employer's control over a telecommuting employee will be considerably less compared to an employee at the actual workplace. The employer will not likely have the ability to supervise and monitor a telecommuting employee as it would an employee in the workplace. Further, telecommuting employees may own their own computers, modems, and fax machines and perform different work than on-site employees. These employees can potentially be viewed as having invested in the equipment and materials necessary to perform their jobs. The ultimate impact on an independent contractor analysis will be seen in time as companies routinely use telecommuting.

Wage-And-Hour Issues

The information superhighway also raises several issues under wage-and-hour law. How does an employer determine and record the hours of work of a nonexempt employee working in his or her home? How will break period and meal period requirements be enforced for nonexempt employees? How will "regular work hours" be established for purposes of determining whether training time is outside such hours and thus, possibly noncompensable? How long must a "break" be for an employee working at home before it becomes noncompensable time? How does an employer monitor and control overtime? How, when, and where will wages be paid? Will travel time to a company facility be noncompensable commute time or compensable travel time between work sites? How will partial days of absence from work be calculated for exempt employees whose employers require use of paid leave in such situations? Should an exempt employee, who logs on his/her computer for five minutes to answer a question from work before leaving for a day of personal business, be paid for a full day's salary? These issues are certainly not insurmountable, but an employer contemplating work by telecommuters needs to address these issues or run the risk of facing considerable liability.

Employers may be subject to additional regulation if the nonexempt telecommuter's work falls within the definition of *homework* as used in the Federal Labor Standards Act (FLSA). Homework is defined as the production of goods "in or about a home, apartment, tenement, or room in a residential establishment," regardless of the source of the materials used by the homeworker. 29 C.F.R. § 530.1(d). Nonexempt employees performing *homework* must be paid minimum wage and overtime as required by the FLSA. The FLSA also has specific recordkeeping requirements applicable to employees performing homework. Further, employers in certain industries must obtain certificates for homework and must fill out an employee handbook that specifies, among other things, the number of hours worked. The FLSA's definition of homework and its corresponding regulations clearly focus on industrial manufacturing employees. The definition, however, is arguably broad enough to include many telecommuters. Employers must consider the impact of these laws on any telecommuting program.

Several states, including California, New York, Connecticut, Hawaii, and Illinois have laws like the FLSA that regulate certain types of work performed in the home. Several of the statutes appear limited in application to homework involving industrial manufacturing. As mentioned in the discussion above, however, many of the statutes are written broadly enough that they may be applied to home technology and the work performed utilizing this technology. The laws vary in the amount of regulation imposed on employees who perform regulated homework. Most of the laws require the employer and the employee to obtain permits and certificates for the homework. Other states, such as Illinois, require that the employee's home work area have proper ventilation and specifies the cubic feet of airspace an employee must have in the work area. Further, most of the statutes require a certain amount of recordkeeping for the homeworker. Employers should consider these state homework laws in relation to their telecommuting programs.

The traditional factors used to determine when *on-call time* is work time will also need to be reevaluated for the nonexempt telecommuters. Federal regulations state that if an employee is required to wait for a call to work at the employer's premises or any location other than the employee's home, all waiting time must be counted as hours worked. The considerations in determining whether on-call time is work time include the employee's freedom of movement, the frequency of calls to return to work, response-time requirements, and equipment transportation. The changing context of the working environment for telecommuters will obviously require alternations in the traditional analysis. (For a complete discussion of wage-and-hour law, see Chapter 27 of The 2000 National Employer®.)

Negligent Supervision

Many states have a cause of action known as negligent supervision. An employer can be held liable for negligent supervision when the employer becomes aware, or should have become aware, of problems with an employee that indicate unfitness but the employer fails to take further action, such as investigating or discharging the employee, and that employee injures a third party. *See, e.g.*, *M.V. By and Through v. Gulf Ridge Council Boy Scouts of Am., Inc.*, 529 So. 2d 1248 (Fla. D. Ct. App. 1988). (For a more extensive discussion of negligent supervision, see Chapters 12 and 34 of The 2000 National Employer®.)

Employers need to be aware that with the increase in virtual workers and virtual teams, the risk of being held liable for negligent supervision also increases. Supervisors have much less control over virtual workers and will find it more difficult to supervise them. Virtual workers may be spread out throughout the world and may never meet with a supervisor face to face.

To supervise virtual workers effectively, employers must have the ability to monitor all online communications. Employers must make certain to implement a policy that clearly allows the employer to monitor all online communication and must make certain to get all virtual workers to consent in writing to such monitoring.

The Identity Of Virtual Workers

An employer who hires a virtual worker may never meet that worker face to face. Thus, the employer must take extra care in verifying that the employee is who he claims he is. One employer who hired virtual workers recently discovered that the workers he thought were residents of Iowa were actually from India and were not authorized to work in the United States. An employer must verify the applicant's résumé before hiring her, and must make sure that all other laws are obeyed. For example, to ensure that no child labor laws are violated, an employer should make certain the applicant is in fact old enough to work. The age of an applicant is easy to discern when an employer meets an applicant, but virtual workers are often never seen by the employer. In addition, an employer must make certain that the virtual worker is authorized to work in the United States.

Workplace Violence

The ever-increasing utilization of remote locations for work may create greater exposure to workplace violence. For instance, employees working in remote locations or in their homes may not have the safety and security of a larger, more public working environment. This may greatly increase employee exposure and, consequently, an employer's liability.

Furthermore, a leading cause of violence in the workplace is domestic disputes that spill over into the working environment. On the other hand, workplace violence problems may be somewhat mitigated by the fact that more of these remote locations may be outside of urban areas where street violence is more prevalent. (For a more extensive discussion of the workplace violence issues and potential solutions, see Chapter 34 of The 2000 National Employer®.)

Collective Bargaining Units

In order to unionize a group of workers, the union must first designate an appropriate bargaining unit that it wishes to represent. Determining the bargaining unit becomes more difficult when dealing with members of a virtual team.

In determining if a unit of employees is an appropriate bargaining unit, the NLRB relies heavily on the "community of interest" test. If a community of interest exists among the employees, they comprise an appropriate bargaining unit. In determining if a community of interest exists, the NLRB considers factors such as common supervision, contact among employees, and common work locations.

These factors are not easily applied to a virtual-team situation. For example, what qualifies as supervision in cyberspace? Virtual team members also have no, or almost no, physical contact with each other and do not have common work locations. Does contact in cyberspace qualify as contact among employees? If all virtual team members work together in cyberspace, do they have a common work location? These questions have not yet been answered by the NLRB, but they will likely be addressed in the near future.

The WARN Act

The Worker Adjustment and Retraining Notification (WARN) Act, 29 U.S.C. §§ 2101-09, requires employers covered by the Act to give employees, unions, and local and state government officials sixty days' notice prior to a plant closing or mass layoff. The Act's requirements are triggered when a mass layoff or plant closing occurs at a "single site of employment."

The Act's reliance on the "single site of employment" concept presents some questions for a business that operates in cyberspace. For example, if a company lays off fifty members of a virtual team that work in fifty different cities, will the fact that they all work together in cyberspace satisfy the "single site of employment" rule? If a company does not have a traditional "site of employment," but works solely in cyberspace, will cyberspace be considered a "single site of employment"? As more companies begin to operate in cyberspace, the answers to these questions will become clearer.

Tips For Implementing A Successful Telecommuting Policy

While telecommuting poses many advantages for both employers and employees, there are important disadvantages as well. For instance, telecommuting is not suitable where face-to-face interaction with colleagues or clients is essential to the job. Telecommuting poses management challenges, from developing a system for communication, to developing ways to assess employee performance. One author suggests that "[a] telecommuting job should have activities that can be measured, be done for the most part independently, be portable to a nonoffice environment, have observable beginning and end points, not need special equipment that is only at the work site, and not have deadline requirements that come from outside the telecommuter's department." George M. Piskurich, *Making Telecommuting Work*, Training & Dev., Feb. 1996. Furthermore, some employees lack the independence and commitment required of successful telecommuters, while others may feel isolated from colleagues, or feel unable to separate their work and personal lives.

These issues raise important questions to consider before implementing telecommuting as an option: How will the employee's quality and quantity of work be monitored? How will the employee's hours of work, including break periods, meal periods and overtime be monitored? How can the use of company equipment be limited to business purposes? If an employee's child spills soda on a computer keyboard, who is responsible for replacing the equipment? How will confidential information be protected? Will a telecommuting policy impact negatively on those employees who must come to the employer's premises?

To ensure a successful telecommuting program, employers are advised to follow these guidelines:

- Choose telecommuters carefully, considering, among other things, an employee's ability to work independently with minimal direct supervision.
- Restrict telecommuting opportunities to those workers with a history of satisfactory performance, and to those who have the necessary skills in qualified job positions.
- Require newly hired telecommuters to spend a period of time in the office first, so that they will develop a sense of corporate style, and so that the employer will have an idea of their abilities.
- Keep in constant contact with telecommuters–schedule weekly meetings, or occasional face-to-face meetings.
- Consider automatic routing of information–technology now permits memos, corporate data, and job-related information to be set up to automatically route or copy to the telecommuter.
- Clear directives, objectives, and deadlines help employers to monitor telecommuters. Many employers with successful telecommuter programs have established a weekly report to communicate progress, problems, and plans. Employers may wish to establish regular in-office days, so that the company knows when to expect the employee.
- Help telecommuters set and recognize their own rewards for completing tasks, as the demands of telecommuting may be unfamiliar to first-time telecommuters. Make sure telecommuters learn to create a balance between the telecommuter's professional life, and personal life; some telecommuters who are not self-disciplined let the personal distractions at home get in the way. Others who are extremely self-motivated and conscientious tend to overwork. Have the telecommuter establish a specific workspace with both physical and mental boundaries. This may mean setting rules for family interruptions.
- Take care to convey the organization's culture and policies–require attendance at orientation sessions, hold mandatory

training sessions at the employer's place of business, and make sure that telecommuters have access to all employment policies, corporate memos, and handbook updates.

Managers, too, must be carefully selected. Managers must learn to evaluate work based on performance and productivity, and to manage the project, not just the person. Supervisors will have to become leaders who help to set goals, plan work, and guide work. Because supervisors can no longer oversee the work process in person, they will have to learn to manage results. Employers may wish to hold special workshops on how to manage telecommuters.

LITTLER'S NINE-PHASE PROCESS FOR REDUCING EMPLOYMENT-RELATED LITIGATION ON THE INFORMATION SUPERHIGHWAY

The vital role of the digital workplace in the reengineering of American business is undeniable and will expand. Every responsible employer in the United States either has or ultimately will experience the tension between new technology and existing employment standards. This tension often arises with the introduction of new technology into the workplace.

New technology is often critical to a company's efforts to stay competitive. However, in the rush to introduce state-of-the-art technology, employers are often willing to overlook any potential problems related to the technology. Employers must anticipate problems and tensions and develop policies and procedures to deal with them. Otherwise, the benefits that arise from the digital workplace could be largely offset by litigation and other costs.

Littler's task force on the digital workplace has developed a process and procedure for introducing new technology into the workplace in a way that can help reduce the potential of litigation. Littler's nine-phase process emphasizes employee privacy concerns. However, recommendations are also provided for other concerns described above, including discrimination claims, employee safety, wage-and-hour concerns, and traditional issues under the National Labor Relations Act.

The focus of the nine-phase process is on developing solutions to the problems outlined above. Employers must recognize that the pace of technological change has been much faster than the development of case law and litigation. More than most areas of employment law, in the digital workplace it is necessary to anticipate the future and be willing to invent policies and solutions before courts have established clear guidelines or, in some cases, any guidelines. Process and planning become necessary substitutes for the more traditional case histories and legislative enactments.

Phase I: Implement New Technology Using A Team Selection Process That Focuses On Employment-Related Issues

Employers often ignore employment-related legal problems that may accompany the introduction of new technology. Many employers focus on the quick implementation of new technology in order to gain the immediate benefits of increased productivity and efficiency. However, in so doing, the employer may not anticipate the effect the new technology may have on personnel policies and procedures or the potential employment-related legal problems that may accompany the new technology. Employers often implement the new technology without even consulting with the human resources or legal departments.

The implementation of a voicemail system is a classic example. Often, the business services department decides that voicemail will improve productivity and reduce costs. This message travels to the CEO who directs that at least three bids will be received to ensure that the best buying opportunity is located. A final decision is then made and a new voicemail system is ordered and installed.

Although this process might be quick and efficient, a key component was missing. No one ever questioned how the new voicemail-system would integrate with current personnel policies and procedures, or wondered what potential legal liabilities might exist with regard to its use and how these liabilities might be limited. In short, the human resources and employment-related legal issues were not given serious consideration in the planning and acquisition process. This departmentalized thinking can be divisive, inefficient, and is usually wrong.

It is essential that today's employer adopt a multidisciplinary approach to implementing new technology. A team should be formed and staffed with representatives from all affected departments, including human resources and legal. The team should be given the goal of implementing technology and integrating the new technology into the business objectives of the organization. The team process will help to ensure that the new technology will either fit existing employment policies or that those policies will be modified coincident with the installation of the new system. In this manner, it is more likely that troublesome issues that could result in litigation will be identified in advance.

The positive effects of a multidisciplinary approach in this area can be substantial. For example, a corporation was forced to settle a lawsuit for millions of dollars because of an alleged hostile work environment claim that emanated from the uncontrolled use of an

electronic bulletin board of a recently installed e-mail program. This problem could easily have been anticipated and avoided with simple access and review procedures.

In addition, Charles E. Grantham, author of The Digital Workplace and one of the foremost authorities on telecommuting in the United States, attributes failure to involve the legal department in the planning phase as one of the major reasons that telecommuting programs fail in the implementation stage or are unsuccessful. There are many other barriers to the success of technological changes. However, failure to involve the human resources and the legal department in the planning and development of these programs is near the top of the list.

Phase II: Review Existing Employment Policies Including Those Governing Workplace Privacy

Once an employer has committed to examining the employment law considerations associated with the introduction of new technology, it is essential to critically review existing policies to determine how technology is addressed by the policies and whether the policies need modification. Review of employee privacy policies is especially important.

Too few employers have developed comprehensive privacy policies. Such a policy is becoming more and more essential, given the growth of privacy litigation, negligent hiring lawsuits, and wrongful discharge actions. Privacy policies should generally regulate issues ranging from control of medical and personnel records to issues of access to personnel records by law enforcement or other quasi-official entities. However, even if a company has a privacy policy, it will probably have to be reviewed to ensure that it addresses issues unique to the digital workplace.

For example, the introduction of an e-mail system raises specific privacy concerns. Can an employee access sensitive medical information and, if so, what controls and limitations can be put in place concerning such information? Who will have access to e-mail messages and are they considered confidential? These issues will need to be addressed in any comprehensive privacy policy.

The review of written policies does not necessarily end the policy review process. Several courts have recognized that past conduct, practices, and unrelated writings can create *de facto* policies and standards. *Kern v. Levolor Lorentzen, Inc.*, 899 F.2d 772 (9th Cir. 1990); *Pugh v. See's Candies, Inc.*, 116 Cal. App. 3d 311 (1981). These company practices and *de facto* policies need to be inventoried and reviewed as part of the process of assimilating new technology.

Phase III: Establish A Self-Auditing & Issue-Spotting Process

In planning for the implementation of new information technology in the workplace, one must consider a wide range of practical and legal employment implications. A sample checklist of questions, developed by Littler's Digital Workplace Taskforce has been provided as Appendix A to this chapter to assist employers in considering a broad range of problems and litigation risks.

This list should be used as a starting point for the team assigned the task of implementing new technology. The team should, at a minimum, consider carefully each of the questions. It is anticipated that the process of answering these questions will suggest additional potential problems and tactics for improving the implementation process.

Phase IV: Develop Practical & Innovative Responses To The Employment-Related Issues Raised By The Introduction Of New Technology

The development of policies is an important and integral step toward facing the new technology. The policies must be as complete, complex, and innovative as necessary to meet the requirements of the new technology. Sample policies have been provided at the end of this chapter as Appendix B.

Each policy directly responds to concerns over employee privacy associated with these technological innovations. Under the issue-spotting process, the organization, it is hoped, will have identified all critical issues associated with the new technology. These issues can then be addressed in policies as privacy is addressed in the sample policies.

For example, with regard to voicemail, issues concerning the expectation of privacy on the part of outside voicemail callers as well as the employee recipients of calls will have been noted. In response, an appropriate policy must be developed that effectively reduces the expectations of privacy; establishes company ownership of the system and the messages; authorizes the organization to access the voicemail; and informs incoming callers that the conversation might be heard by someone other than the person whose voicemail was activated. By creating such a policy and later explaining it to employees, the company fully discloses to employees and callers what they can expect, which minimizes the potential for a later legal challenge.

The development of practical responses and solutions are as varied as the problems that arise. For example, sexually explicit messages on an e-mail system may later serve as evidence in a sexual harassment case. Within the e-mail sample policy, a prohibition is included with regard to certain discriminatory or offensive language. This effectively integrates e-mail into the company's existing sexual harassment policy. It also ensures the enforceability of the sexual harassment policy as applied to e-mail.

Phase V: Develop A Training Program To Implement Digital Workplace Policies

The self-directed workforce and the elimination of several levels of supervision have created an environment in which the role of training has taken on a higher level of importance. The regulations and policies related to new technology become the tools for managers to avoid future litigation problems. Training managers concerning the proper use and misuse of new technology is paramount to reducing litigation risk. In many areas, this training will extend beyond the managers to the employees who utilize and access the technology.

Again, voicemail and e-mail are prime examples of this principle. Managers should be trained regarding the rules governing access to the systems and the rules regarding the type of information that can be transmitted electronically through these channels. As part of learning how to use the new technology, employees should also receive instruction regarding these rules and regulations. The additional burden of this type of training will be almost negligible as new technology, by definition, requires training for its implementation.

If litigation develops in the future, policies and training will provide the best possible evidence regarding the employee's expectation of privacy and will establish that the employer demonstrated a standard of care. Again, the key is to include a component within the normal training programs associated with the new technology that focuses on employment law considerations. This reaffirms the need for a multidisciplinary approach, the breakdown of departmental lines, and the need for advance planning.

The failure to adequately train users of new technology could result in substantial liability for negligent training. If, for example, an employee is not properly trained and inadvertently disseminates private personal information through an e-mail or voicemail system, there could be a claim of negligent training resulting in an actionable invasion of privacy. Similarly, if an inadequately trained employee were to lose, destroy, or misrecord vital information needed by a customer or someone else outside of the company, the failure to train could result in a tort claim for negligent training. Moreover, the failure to properly train employees in the safe use of technology and in ergonomic considerations could also result in injuries to the employees using the system for which the employer would be responsible through the workers' compensation system. All of these additional potential sources of liability provide the motivation necessary to encourage employers to establish a careful program of both initial and ongoing training.

Training in this area will require a multidisciplinary approach. As Diane B. Hartman, president of Quality Training International, recently stated regarding e-mail training:

> Employers are giving a powerful information tool to their employees without directions. Having been swept up in the technical aspects involved, most employers leave e-mail training to computer specialists without involving the HR department. Part of the challenge employers face is having little legal precedent and few effective policies to draw from.

Phase VI: Monitor Policies & Programs To Reduce Employment-Related Litigation Associated With New Technology

Every employer has an obligation to monitor and enforce the policies that govern its workplace. An organization cannot fully meet its key legal obligations by merely providing competent policies and good training. Our liability system is still built on the assumption that the workplace is controlled by the employer and that the employer has a responsibility to monitor and enforce its policies. *Baker v. Weyerhauser Co.*, 903 F.2d 1342 (10th Cir. 1990); *Campbell v. Leaseway Customized Transp., Inc.*, 484 N.W.2d 41 (Minn. Ct. App. 1992); *Duldulao v. St. Mary of Nazareth Hosp. Ctr.*, 115 Ill. 2d 482 (1987). New technology can greatly assist in this process. Unfortunately, it can also create the potential for systematic abuse. In carrying out the duty of monitoring and enforcing employment policies, we recommend consideration of the following:

Technology should be looked at as a potential vehicle for monitoring and enforcing employment law policies and procedures. For example, technology can assist an employer in becoming consistent in its disciplinary decisions. Cases often turn on whether the employer applied the same discipline to similar situations in the past. As new technology provides instant bridging of informational gaps within the organization, consistency becomes a very real possibility.

An employer should monitor employees' use of the new technology to ensure that established policies are followed. For example, one of the common complaints regarding electronic bulletin boards is the posting of obscene material, inappropriate material, or

potentially defamatory material. Most bulletin boards have procedures whereby a manager can remove information. In some organizations, individuals devote their entire working time to reviewing e-mail messages to ensure that they meet company standards and do not violate appropriate guidelines. This type of monitoring can be extremely burdensome yet, in some organizations, absolutely necessary.

The New Jersey Department of Environmental Protection uses its technology to police its employees in one key area–game playing. The Department prohibits employees from playing games such as solitaire on their computers while at work. The Department has a computer program that monitors employee game playing and that displays the following message to violators: "Sorry, department policy prohibits the use of this program" each time an employee attempts to play a game. The mere knowledge on behalf of employees that the employer is monitoring what program is running on their computers is usually enough to significantly curtail such abuses. No one said the monitoring will be easy. Many games now come with *boss keys* designated to hide games behind phony spreadsheets or other documents on the touch of a key.

In addition, an employer should monitor the type of information stored on the system and determine who should have access to the stored information. An organization that stores personnel records on its electronic communications system needs to ensure that there are well-structured safety mechanisms to prevent the flow of this information into inappropriate terminals. The mere existence of certain information creates a litigation risk.

Monitoring and enforcement processes can be greatly enhanced by the creation of a duty to report misconduct. In the sample e-mail and voicemail policies attached to the end of this chapter, such a duty is set forth. Under these circumstances, an individual viewing sexually explicit information on his or her computer screen will have an affirmative obligation to report it to the company. This obligation removes excuses that employees sometimes use for not reporting obscene messages.

If anyone doubts the importance of monitoring, these doubts should have disappeared on April 4, 1994. On that day, most of the major newspapers in the nation reported the arrest of a computer-company employee for illegal sexual activity. A twenty-seven-year-old man allegedly used an electronic bulletin board to solicit sex from a fourteen-year-old boy. The claimed criminal activity was discovered when the father reviewed his son's computer records and saw explicit sexual material. Fortunately, the material was not encrypted. Unfortunately, abuse of the information superhighway in the office and at home is not isolated.

Excerpted below are segments from the March 1994 issue of *BYTE*. Attorney Victor J. Cosentino wrote on what he labels "virtual legality." He observes that, "Once online, some people totally disregard legally and socially acceptable behavior." Cosentino chronicles abuses from privacy violations to formulation of unenforceable contracts. He concludes that, "Employers may be responsible for their employees' forays in this legal miasma." The commentary ends with the following stirring paragraph:

> The truth is that, as individuals, we are responsible for what we do. Since there's no reason to believe that the rate of technological change will slow down or the law will catch up, as users we must become attuned to the legal, social, and ethical ramifications of what we do online. We can lose money in an unenforceable contract. We can hurt and defame people and possibly become legally liable. We can have our privacy breached or our words censored, taken out of context, twisted, or falsified. The solution is to treat the virtual world like the real world, because it is. To believe otherwise makes the likelihood of encountering virtual legality a virtual certainty.

Phase VII: Establish Disciplinary Standards & Procedures Applicable To The New Technology

The misuse of the digital workplace is already an area where employers are facing disciplinary decisions. Employers have the choice of responding to situations as they arise or establishing standards for disciplinary action. Regardless of the approach, consistency will be important to reducing the likelihood of litigation and to ensuring acceptance of the employer's disciplinary process. For example, if an Asian employee accesses a coemployee's e-mail and is terminated, while a white employee is only given a disciplinary warning for the same actions, this could lead to litigation.

Problems of documentation or proof in disciplinary decisions will be both helped and hindered by the new technology. Recently, at a mediation, a manager adamantly denied that he had done anything wrong whatsoever throughout his entire career. The employer then presented the transcript of a voicemail message in which the manager had asked a secretary to falsify an expense report. The transcript and subsequent recording of the voicemail totally changed the direction of the mediation and precipitated a resolution of the dispute. Without a policy that allowed for the accessing of that information and the use of it, a very different outcome could have occurred.

Disciplinary investigations can extend beyond the length of one's employment. Consider the following report from attorney J. Rob

Betts, *Voice Mail and Electronic Mail Messages: A New Battleground For Employee Privacy Disputes*, Calif. Emp. Law Quarterly, Winter 1993, p. 1:

> In late 1992, Eugene Wang, a key vice president of a Silicon Valley software firm, left his company, Borland International, to go to a competitive software firm, Symantec Corporation. A Borland employee tipped the company that Wang had been collecting proprietary Borland information during the past few weeks. Borland elected to search Wang's computer and found a dozen electronic mail messages containing highly confidential information that had been sent by Wang to the CEO of Symantec. The electronic mail system involved was MCI Mail, which is a service allowing electronic mail messages to be transmitted to and from members of the service regardless of where they live or work.
>
> The electronic mail messages contained plans for future Borland software products, lists of salaries of key personnel and prospective business partners and recruits. Based upon these findings in Wang's electronic mail, Borland sued Wang and Symantec, alleging misappropriation of trade secrets and related claims. Borland also convinced a local judge to issue search warrants for the homes and offices of Wang and the CEO of Symantec. Additional incriminating documents were found in the possession of each, and criminal indictments were handed down against these two individuals.

Preexisting policies and standards are essential in the proper handling of disputes such as the one described above.

Turning to practical solutions to potential discipline, Littler strongly recommends the consideration of an alternative dispute resolution (ADR) technique, including mediation and arbitration. If discipline is taken against someone for violating an e-mail policy or based on information provided through advanced technology, it will be to everyone's advantage to have it resolved without formal litigation. ADR presents an option for accomplishing this, it is hoped, through mediation and a voluntary resolution. If this is not possible, then arbitration becomes a final option.

Phase VIII: Use Multidisciplinary Innovations To Solve Problems Related To New Technology

A traditional process of analyzing potential employment law issues has been set forth above. That process includes spotting issues, developing responses, training managers and employees regarding their duties and responsibilities, monitoring the system for violations and then taking appropriate disciplinary action. These traditional steps, however, all take place within the company's own organization. They do not necessarily contemplate a multidisciplinary approach that may provide solutions to employment law considerations ranging beyond the traditional tools of a human resources department or corporate counsel.

The use of other disciplines such as psychology, sociology, or informational and organizational specialties may provide useful perspectives that can have an immeasurable impact on the digital workplace. One of the best examples of this is telecommuting. A review of telecommuting demonstrates that there are numerous legal problems. An individual working at home, who is nonexempt, faces several wage-and-hour concerns. How is time recorded? What constitutes working time? What is the workday? How does the employer ensure that the work is, in fact, done during the hours specified by the employee?

Although the legal problems are important, the legal discipline only touches the edges of a full range of issues that affect a telecommuting program. For example, psychologists talk about social isolation and a feeling of being out of the mainstream. Over-monitoring? Under-monitoring? Depression associated with isolation? Information and organizational systems specialists are concerned with the effect of the technology on the culture of the organization. How will the structure of the organization change? How will the changes effect communication within the company? All of these issues can be critical to the success of a telecommuting program.

Multidisciplinary and technologically oriented solutions have tremendous potential for solving these types of problems in the workplace. The key ingredient is the participation of individuals from a variety of disciplines in assessing a particular technology and its application to the workplace and keeping in mind the employment law implications as that process occurs.

Phase IX: Maintain A Legislative Watch

It is possible that an organization can follow the above steps and provide an excellent preventive program for the integration of new technology with minimal negative consequences. Unfortunately, these efforts can be derailed if legislative enactments occur without full appreciation of their impact. For example, Congress has considered an electronic-monitoring bill that is designed to eliminate abuse of employee privacy.

Ironically, such legislation could have totally unexpected consequences. For example, an electronic inventory system may be in use that indirectly identifies the exact productivity of each worker within a warehouse. The purpose for the technology is to ensure that the customer can access materials in record time and that the inventory of the warehouse is maintained consistent with the needs of the customer. However, the secondary effect is to provide excellent information on the productivity of the workforce and help dictate the size and training of that workforce. A bill that banned monitoring could inadvertently prohibit this type of warehouse control and severely injure the significant productivity advances that have been made by the application of the new technology.

Employers have a vested interest in making their thoughts and concerns known through their associations regarding the implication of such legislation. Organizations like the American Electronics Association, the United States Chamber of Commerce, and many others have devoted attention to technology-oriented legislation and its employment law implications. An excellent example of such legislation is in the area of encryption and law enforcement access through portholes in the clipper chip. Total encryption could result in money laundering and/or violation of company policies with no redress available to law enforcement or to the employer. The creation of superprivacy, through either technology or legislation, could have tremendous negative consequences on the ability of employers to maintain the type of controls that are otherwise mandated by statutes and regulations within the workplace.

NINE PRACTICAL RECOMMENDATIONS FOR WORKING WITH THE INTERNET WHILE MEETING EMPLOYMENT LAW REQUIREMENTS

One: Develop & Implement A Comprehensive Internet Policy For Your Workplace

During the last five years e-mail and voicemail policies have become commonplace. It is now time to establish an Internet use policy. This can be incorporated into a comprehensive technology policy for the workplace or established as a stand-alone policy. Sample provisions appear at the end of this chapter. An Internet-use policy is more than a good idea, it is a legal necessity. Employees must understand how the employer intends for the Internet to be used in the workplace. Can an employee visit amazon.com during a break using the Company computer and Internet connection? What sites can be visited? When? What material can be downloaded?

A comprehensive Internet policy will help answer the above questions and many more. However, it is insufficient to merely have a well-developed policy. The policy needs to be implemented, explained, and available. Fortunately, the Internet provides a channel for making the policy available and answering questions about it.

Failure to immediately consider and adopt an Internet use policy is the equivalent of failing to renew your organization's liability insurance policy. The difference is that the tuition for your Internet use policy is no greater than the cost of your time to read and apply this chapter and have it reviewed by your corporate counsel.

Two: Conduct A Cyberuse Audit Of Your Internet Systems

In developing the above policy and determining its implementation and enforcement, it is necessary to define how the Internet is being used in your current workplace and its business purpose. Each organization is unique while at the same time has many common problems. An audit provides an introduction to what will be required. Sample questions include the following: How many employees have access to the Internet? Is this always through company-provided computers? Are employees using the Internet through home computers, but for company business? How much time do your employees spend on the Internet? (You may be surprised by the answer.) How well defined are the business objectives associated with Internet use? Is the Internet use unrestricted? Is there any legitimate reason why employees would be visiting sexually explicit Web sites? What requests for Internet access has the company received? What complaints have been reported? What commercial activities are taking place on the Internet as authorized by the company? What security precautions have been developed? Is there training on the use of the Internet? What are the privacy expectations of your workforce? How were these expectations shaped? Are Internet materials routinely downloaded? How are they distributed (if this occurs)? What plans exist for an expanded role for the Internet during the next six months? The next year? Beyond? Is there a plan to use voice recognition software? How are disabled users accommodated? Is encryption available? How do employees identify themselves? Can employees use the Internet without giving their identity? If a Web site is reached that requires a credit card for access, can the employee use a personal card and seek reimbursement? Is a manager's authority necessary to make a payment over the Internet? Who maintains the company Web site? How is the Web site integrated into the operations of the company? Is training offered over the Internet? What health and safety issues have been identified with Internet use?

It is recommended that before such an audit is activated, your corporate attorneys evaluate the implications of collecting the above information. Recognize that if the information is not privileged a plaintiffs' attorney could subpoena the results (*e.g.*, to show that disabled workers are not accommodated as required by the ADA).

Once collected, the audit information provides the basis on which an action plan can be developed. Additionally, an existing policy

can be modified or an initial policy created based on the current treatment of the Internet. Most importantly, such a review will likely identify the areas where abuse is occurring and suggest the need for corrective action.

Three: Conduct An Internet Use Training Program

Organizations routinely have training sessions concerning the proper use of software. A program on how the company envisions the use of the Internet in the workplace should be included in one or more of these sessions. This program should include a review of the Internet policy and a hands-on demonstration of the power of the Internet. A copy of the agenda for the program as well as each participant's receipt of the policy should be documented. If a violation of the policy occurs, the employee will be on record as having received the policy and having had an explanation of what was expected and prohibited. The most important benefit of this process is that employees will use the Internet in a manner intended by the company. The secondary benefit is the ability to discipline employees should that become necessary.

Essential learning programs are currently available through in-person instruction and train-the-trainer sessions. In the near future, training programs will be available over the Internet on how to lawfully use the Internet. See, for example, the course offerings of Employment Law Training, Inc. (ELT) (www.elt- inc.com).

Four: Consider Establishing A Cyberpatrol For The Internet

Having established a state-of-the art Internet policy and educated the workforce on its provisions, the policy requires enforcement. It is certain that abuses will occur and that counseling or corrective discipline will be required. One method of anticipating this problem is to limit Internet access to certain sites and types of materials. Software can accomplish this task and is recommended. Beyond this, the organization may wish to periodically monitor Internet access to ensure that it is appropriate and being used efficiently. Whether this is done as part of the normal duties of management or through a specially trained group of human resource professionals (a cyberpatrol) is dependent upon unique considerations within the organization. Generally, new legal standards will demand some form of prudent "preventive effort" by management as part of later providing an affirmative defense to a charge that misuse of the Internet has created a hostile work environment.

Five: Establish Uniform Standards Of Enforcement For Your Internet Policy

We recommend establishing standards of expected behavior and responses before the inevitable abuses occur. It is imperative that these standards of expected behavior are consistently enforced. Often, different managers enforce workplace policy requirements in different ways. This inconsistency between managers can lead to liability for employers. Also, a single manager may enforce workplace policy requirements one way when dealing with a particular employee and an entirely different way when dealing with another employee. For example, an outstanding producer who is Internet-savvy may be allowed to surf the net without complaint, while a marginal performer is disciplined for nonwork-related use of the Internet. This inconsistent treatment may become a major problem when one of the workers is a minority or in a protected category and the other is not. This creates a presumption that the different treatment may have been the result of discrimination rather than recognition of extraordinary performance. Preestablished standards of performance will help overcome this problem. If a situation arises in which a modification of these standards becomes necessary, the manager and the human resource professionals should be aware that they need to document a nondiscriminatory basis for such a modification.

Six: Brainstorm The Power Of The Internet As An Employment Law Compliance Tool

Schedule a two-hour session for key professionals in your organization responsible for employment law compliance. This session will be for the purpose of exploring how the Internet could reduce your exposure to employment-related litigation. The meeting could occur in a conference room or over the Internet/intranet; however, making it attorney-client privileged is recommended. Ideal participants would be a top human resources representative, corporate counsel, head of security, a representative from IT, a top management representative (hopefully, one with some financial authority), a risk management representative (if such a department exists), head of corporate compliance programs (if such a department exists), and a line management representative. In preparation for the meeting, a designated internal Internet expert should assemble a list of possible ways the Internet could be used for employment law compliance. The meeting should involve a discussion of these applications and end with an action plan.

Possible applications are endless. Selected topics for the agenda could include: Identifying useful Web sites that contain employment law information; using the Internet to distribute necessary policies and information for employees, using the Internet to receive complaints, using the Internet for expert, management, and employee training on employment law (*e.g.*, examine the five Internet Employment Law Compliance courses currently presented by Littler Mendelson and made available through Employment Law Training, Inc.), tracking employee performance, utilizing Internet evaluation forms, using the Internet to support hiring, linking through

the Internet to a real-time background-checking service, making disciplinary information available in order to ensure consistent treatment of employees, using the Internet to make reasonable accommodations, preventing the abuse of the Internet in hiring virtual employees, and privacy concerns raised by Internet use in the workplace.

The full agenda could be developed through a careful reading of this chapter combined with a comprehensive assessment of the special needs and demands of your organization.

Seven: Build A Library Of Useful Employment Law-Related Web Sites

Several of the governmental enforcement agencies have established useful Web sites that provide technical compliance information. We recommend that someone knowledgeable about the Internet and familiar with your compliance needs undertake building a list of Web sites for use in employment law compliance. This list could include approved recruiting sites and sites with a legal focus that could be of use to corporate counsel. Such a list could become the size of a small-town phone directory in a short time. Accordingly, we recommend limiting the list to categories and only a few preevaluated sites. This will better ensure that quality information is being received. Sites that are not updated regularly and therefore have out-of-date information should be eliminated from the list.

A few suggested sites are included in the above chapter. Periodically, Littler Mendelson will provide suggestions; however, there is no substitute for your own professional investigation.

Eight: Answer The User-Identification Challenge Of The Internet

One of the major employment law related challenges of the Internet is being able to identify who is doing the communicating. Did employee John Doe actually receive a corporate antiharassment policy? Who sent the obscene e-mail that originated via <www.anoymizer.com>? Was a manager's password used by an angry former employee? These and many more critical questions turn on establishing the identity of the Internet user.

Human resources and corporate counsel should be involved with IT in establishing the level of technology used to prove identity within the organization when using the Internet. Incredible tools are now available ranging from codes which can only originate from your computer to cybersignatures and beyond. If ultimate security is needed, fingerprint systems and retina scans are becoming more available at almost affordable prices.

The identity challenge is a formidable one facing today's employers. Your organization's response to this challenge needs to be decided rather than left to be answered by inaction.

Nine: Identify & Train Your Internet Expert Witness For Personnel-Related Issues & Employment Law Litigation

The practical goal of considering the Internet in the context of current employment and labor laws is to avoid litigation and create the type of working environment which will support rather than hinder productivity. Nonetheless, there is a need to have an articulate "expert" within the organization who understands the Internet. This individual should be trained in employee investigations and be schooled in cybersabotage. Her or his role will be to aid the human resources and legal departments in all aspects of Internet employment law compliance. The Internet expert can also offer advice on how the Internet can be used as a productive tool in preventive efforts. When abuse occurs, this Internet expert will be invaluable in defining what can be technologically established and how to identify the offending parties. If disciplinary action is taken and is later challenged, this person will be the logical witness to explain how the organization followed legal requirements. Moreover, an Internet expert will be able to explain complicated technology to a court, administrative hearing officer, or jury in a way that it can be understood.

Another role for this person will be the building of a prelitigation compliance evidence package. This will include a description of employment law compliance action that can be used for the media or the courtroom in showing that the organization took reasonable care to ensure compliance (independent from the specifics of a particular case in controversy).

CONCLUSION

The ultimate effect that the development of the information superhighway will have on the workplace remains to be seen. However, employers need not wait until the highway is complete to begin their travels. Employers who wait for legislation or the courts to define the parameters of the highway before acting will encounter costly, time-consuming roadblocks. We hope the process described above and the sample policies attached will enable the employer to better navigate the digital workplace and decrease the risk of litigation in the process.

***Reprinted with permission,**

Chapter 23 of The 2000 National Employerâ

APPENDIX A:
Planning For Technology Implementation
Twenty Questions Checklist

1. What is the nature and the purpose of the new technology, and what is the goal in introducing it into the workplace? How will these issues be communicated to the workforce?

2. Should the company place limits of the uses of the new technology, and if so, what limits will be imposed? How will these goals be communicated and enforced?

3. Who will be the authorized users of the new technology, and how will they be identified within the company?

4. Will there be sensitive or confidential business or personnel information available in or transmitted through the system?

5. What steps, including policies, procedures, and technical protective systems, should be established to protect confidential and business information? How will access to sensitive information in the new system be limited to those with a legitimate need to know?

6. In what ways is the new technology vulnerable to unauthorized access or sabotage by employees, and what steps can be taken to prevent this?

7. Will the company monitor or access the information stored or transmitted by employees? If so, how will notice of this access and monitoring be provided to the employees?

8. Will employees be asked to sign authorizations for electronic access and monitoring? If so, what should be the contents of the authorization and the procedure for signature?

9. Which of the company's personnel policies will need to be revised in light of the new technology?

10. What training will be required and/or offered to employees concerning the new technology?

11. Will there be safety and occupational health training needed as a result of the new technology? Will existing safety and health programs need to be revised?

12. What potential health or safety problems may be presented by the new technology, and how will the company address those potential problems? What ergonomic

accommodations should be offered to employees using the new technology?

13. What procedures or protections will be established to prevent misuse of the new technology, such as harassment or discrimination?

14. Will the new technology enable employees to work at home? If so, what new policies and procedures will be needed to handle supervision, training, compensation, workplace safety, and other employment issues for employees working at home?

15. How will work time, recordkeeping, break times, scheduling, and overtime be handled for employees working in the home?

16. Will existing employees be retrained to use the existing technology, or will new employees be hired? Will any existing jobs be eliminated? What about employees who cannot be trained on the new technology or who refuse such training?

17. Will the new technology require any special accommodations for existing employees with disabilities? Will it permit special accommodations for disabled employees that were not available before?

18. What steps, policies, or procedures will be used to prevent employees from encoding or encrypting information stored or transmitted using the new technology? What steps will be taken to prevent anonymous transmission or data entries?

19. What criteria will be used to evaluate employees using the new technology, and should the compensation or performance evaluation systems be modified in any way?

20. Will the new technology affect the working condition of any employees represented by a union, and if so, will the union be notified or consulted? Is there a statutory duty to bargain with the union over any aspect of the new technology?

APPENDIX B:
Sample Provisions to be Included in a Policy Regarding Use of Technology & the Internet

Introductory Provision

The company's technical resources–including desktop and portable computer systems, fax machines, Internet and World Wide Web (Web) access, voicemail, e-mail, electronic bulletin boards, and its intranet–enable employees quickly and efficiently to access and exchange information throughout the company and around the world. When used properly, we believe these resources greatly enhance employee productivity and knowledge. In many respects, these new tools are similar to other company tools, such as stationery, file cabinets, photocopiers, and

telephones. Because these technologies are both new and rapidly changing, it is important to explain how they fit within the company and within your responsibilities as an employee.

This policy applies to all technical resources that are owned or leased by the company, that are used on or accessed from company premises, or that are used for company business. This policy also applies to all activities using any company-paid accounts, subscriptions, or other technical services, such as Internet and Web access, voicemail, and e-mail, whether or not the activities are conducted from company premises.

Warning

As you use the company's technical resources, it is important to remember the nature of the information created and stored there. Because they seem informal, e-mail messages, voicemail messages and messages posted on the Internet are sometimes offhand, like a conversation, and not as carefully thought out as a letter or memorandum. However, even after you delete these messages or close a computer session, the information may still be recoverable and may even remain on the system. You should keep this in mind when creating e-mail messages, voicemail messages, messages on the Internet, and other documents on the computer.

Acceptable Uses

The company's technical resources are provided for the benefit of the company and its customers, vendors, and suppliers. These resources are provided for use in the pursuit of company business and are to be reviewed, monitored, and used only in that pursuit, except as otherwise provided in this policy.

[Optional Paragraph: Employees are otherwise permitted to use the company's technical resources for occasional, nonwork purposes with permission from their direct manager. Nevertheless, employees have no right of privacy as to any information or file maintained in or on the company's property or transmitted or stored through the company's computer, voicemail, e-mail, or telephone systems.]

Unacceptable Uses

The company's technical resources should not be used for personal gain or the advancement of individual views. Employees who wish to express personal opinions on the Internet are encouraged to obtain a personal account with a commercial Internet service provider and to access the Internet without using company resources. Employee postings are not permitted on the company's intranet or electronic bulletin board.

Solicitation for any noncompany business or activities using company resources is strictly prohibited. Your use of the company's technical resources must not interfere with your productivity, the productivity of any other employee, or the operation of the company's technical resources. Employees may not play games on the company's computers and other

technical resources. Employees may not access nonbusiness-related Web sites or commercial Web sites unless necessary for business purposes and authorized by their direct manager.

You should not send e-mail or other communications that either mask your identity or indicate that they were sent by someone else. You should never access any technical resources using another employee's password. Similarly, you should only access the libraries, files, data, programs, and directories that are related to your work duties. Unauthorized review, duplication, dissemination, removal, installation, damage, or alteration of files, passwords, computer systems or programs, or other property of the company, or improper use of information obtained by unauthorized means, is prohibited.

Sending, saving, or viewing offensive material is prohibited. Messages stored and/or transmitted by computer, voicemail, e-mail, or telephone systems must not contain content that may reasonably be considered offensive to any employee. Offensive material includes, but is not limited to, pornography, sexual comments, jokes or images, racial slurs, gender-specific comments, or any comments, jokes, or images that would offend someone on the basis of his or her race, color, creed, sex, age, national origin, or ancestry, physical or mental disability, veteran status, as well as any other category protected by federal, state, or local laws. Any use of the Internet/Web, intranet, or electronic bulletin board to harass or discriminate is unlawful and strictly prohibited by the company. Violators will be subject to discipline, up to and including discharge.

The company does not consider conduct in violation of this policy to be within the course and scope of employment or the direct consequence of the discharge of one's duties. Accordingly, to the extent permitted by law, the company reserves the right not to provide a defense or pay damages assessed against employees for conduct in violation of this policy.

Access To Information

The company asks you to keep in mind that when you are using the company's computers you are creating company documents using a company asset. The company respects the individual privacy of its employees. However, that privacy does not extend to an employee's work-related conduct or to the use of company-provided technical resources or supplies.

The company's computer, voicemail, e-mail, or telephone systems, and the data stored on them are and remain at all times the property of the company. As a result, computer data, voicemail messages, e-mail messages, and other data are readily available to numerous persons. If, during the course of your employment, you perform or transmit work on the company's computer system and other technical resources, your work may be subject to the investigation, search, and review of others in accordance with this policy.

All information, including e-mail messages and files, that is created, sent, or retrieved over the company's technical resources is the property of the company, and should not be considered private or confidential. Employees have no right to privacy as to any information or file

transmitted or stored through the company's computer, voicemail, e-mail, or telephone systems. Any electronically stored information that you create, send to, or receive from others may be retrieved and reviewed when doing so serves the legitimate business interests and obligations of the company. Employees should also be aware that, even when a file or message is erased or a visit to an Internet or Web site is closed, it is still possible to recreate the message or locate the Web site. The company reserves the right to monitor your use of its technical resources at any time. All information including text and images may be disclosed to law enforcement or to other third parties without prior consent of the sender or the receiver.

Confidential Information

E-mail and Internet/Web access are not entirely secure. Others outside the company may also be able to monitor your e-mail and Internet/Web access. For example, Internet sites maintain logs of visits from users; these logs identify which company, and even which particular person, accessed the service. If your work using these resources requires a higher level of security, please ask your manager or the IT department for guidance on securely exchanging e-mail or gathering information from sources such as the Internet or World Wide Web.

All employees should safeguard the company's confidential information, as well as that of customers and others, from disclosure. Do not access new voicemail or e-mail messages with others present. Messages containing confidential information should not be left visible while you are away from your work area.

E-mail messages containing confidential information should include the following statement, in all capital letters, at the top of the message: CONFIDENTIAL: UNAUTHORIZED USE OR DISCLOSURE IS STRICTLY PROHIBITED.

Security Of Information

Although you may have passwords to access computer, voicemail, and e-mail systems, these technical resources belong to the company, are to be accessible at all times by the company, and are subject to inspections by the company with or without notice. The company may override any applicable passwords or codes to inspect, investigate, or search an employee's files and messages. All passwords must be made available to the IT Department upon request. You should not provide a password to other employees or to anyone outside the company and should never access any technical resources using another employee's password.

In order to facilitate the company's access to information on its technical resources, you may not encrypt or encode any voicemail or e-mail communication or any other files or data stored or exchanged on company systems without the express prior written permission from the IT department and your manager. As part of this approval, the IT department will indicate a procedure for you to deposit any password, encryption key or code, or software with the IT department so that the encrypted or encoded information can be accessed in your absence.

Copyrighted Materials

You should not copy or distribute copyrighted material (*e.g.*, software, database files, documentation, articles, graphics files, and downloaded information) through the e-mail system or by any other means unless you have confirmed in advance from appropriate sources that the company has the right to copy or distribute the material. Failure to observe a copyright may result in disciplinary action by the company as well as legal action by the copyright owner. Any questions concerning these rights should be directed to your manager.

The Company's Software Policy

If you want to install software on company computers, you must contact the IT department and request to have the software installed. Employees are prohibited from installing any software on any company technical resource without the express prior written permission of the IT department.

Involving the IT department ensures that the company can manage the software on company systems, prevent the introduction of computer viruses, and meet its obligations under any applicable software licenses and copyright laws. Computer software is protected from unauthorized copying and use by federal and state law; unauthorized copying or use of computer software exposes the company and the individual employee to substantial fines and exposes the individual employee to imprisonment. Therefore, employees may not load personal software onto the company's computer system and may not copy software from the company for personal use.

The company will cooperate with the copyright holder and legal officials in all copyright matters.

Your Responsibilities

Each employee is responsible for the content of all text, audio, or images that they place or send over the company's technical resources. Employees may access only files or programs, whether computerized or not, that they have permission to enter.

Violations of any guidelines in this policy may result in disciplinary action up to and including termination. In addition, the company may advise appropriate legal officials of any illegal violations and cooperate in investigations conducted by legal officials.

*** Reprinted with permission, Chapter 23 of The 2000 National Employerâ publication**

APPENDIX C:
Components Of A Successful

Telecommuting Policy

1. The company's responsibilities under the Telecommuting Agreement.
2. The employee's responsibilities under the Agreement.
3. Visits by the employer to the telecommuter's off-site location.
4. Wages.
5. Benefits.
6. Hours/overtime. Work hours. Scheduled workweek.
7. Vacation.
8. Training.
9. Phone contact procedures defined, and arrangement for the handling of calls made by the telecommuter from the remote work location for company business.
10. Termination of Agreement.
    a. Termination–return of equipment, records.
    b. Termination–will the telecommuter's travel to the company's office for purpose of returning office equipment be considered working time?
    c. Will the company reimburse the employee for such travel?
    d. If telecommuter fails to return company-owned equipment, software, records, etc.
11. Safety.
    a. Liability for Injuries.
    b. Who is responsible for designing and maintaining the workplace, free from hazards?
    c. Who will ensure that workplace complies with all occupational safety and health standards and regulations?
    d. Telecommuter's home must be up to the local building code.
    e. Who is responsible for setting up and maintaining an ergonomically correct workstation?
    f. Workplace violence policy.

12. Telecommuter responsibility for any tax implications related to his or her home workspace.
13. Equipment.
    a. List of equipment provided by company.
    b. Telephone lines–will they be in the company's name?
    c. Is the company responsible for installation, repair, and maintenance of company-owned telecommuting equipment and furniture?
    d. Liability for damage to equipment, furniture.
    e. Handling of technical problems with home computers/equipment.
    f. Safekeeping records–fireproof safe.
14. Confidentiality.
    a. Don't release to telecommuter's family.
    b. Fireproof files.
    c. Lock away all documents at end of each day.
    d. Mark documents as confidential.
    e. Requirements and techniques for computer information security.
15. Performance expectations.
16. Documentation of due dates and assignments.
17. Internet, World Wide Web, and company's Intranet policy.
18. Telecommuter responsibility for the content of all text, audio, or images that he or she places or sends over the Internet.
19. Use of company password to express personal opinions on the Internet.
20. Harassment and discrimination policies.
21. Employee reimbursement procedures.
22. Signed agreement.

SFRDOCS:30326723.1 800000.1000

09/20/00 2:28 PM