Cal/OSHA, DOT HAZMAT, EEOC, EPA, HIPAA, IATA, IMDG, TDG, MSHA, OSHA, Australia WHS, and Canada OHS Regulations and Safety Online Training

This document is provided as a training aid and may not reflect current laws and regulations.

Be sure and consult with the appropriate governing agencies or publication providers listed in the "Resources" section of our website.

www.ComplianceTrainingOnline.com

Workplace e-mail and Internet use: employees and employers beware

An employee's personal use of an employer's e-mail system and of Internet access is not protected under the law, and employers can face legal liability for employees' inappropriate use thereof

Charles J. Muhl

The widespread use of the Internet and electronic mail ("e-mail") has transformed the way business is conducted in the typical American workplace. Written communication to almost anyone in the world now can be completed nearly instantaneously; information about any subject encountered in a daily job task can be retrieved in seconds from the Internet through multiple search engines. These technological developments have benefited employers and employees alike—employers in accomplishing business goals and employees in performing their duties.

Undoubtedly, the Internet and e-mail also have given employees a new means of escaping briefly from long days at the office. What sports enthusiast, for example, hasn't taken a quick peek at ESPN.com on the Internet during working hours to see the latest sports news? Who hasn't interrupted his or her work for a moment to send a quick note to a friend about the coming weekend's social events?

A recent extensive survey[1] of employers and employees to gauge their opinions on Internet and e-mail use at the workplace revealed that both groups view non-work-related use of the Internet and e-mail as appropriate, even though, in their mutual opinion, such use may hinder employees' productivity. As a general matter, most employees believe that some personal Internet or e-mail use at work is acceptable and that employers should not have the right to monitor what sites employees are visiting or what e-mails they are sending and receiving. More than 87 percent of employees surveyed stated that it was appropriate for them to surf non-work-related Web sites for at least some portion of the workday. Of these, some 55 percent indicated that it was appropriate for employees to spend anywhere from 15 minutes to 30 minutes on the Internet or dealing with personal e-mail each workday. Nearly 84 percent of the employees surveyed indicated that they regularly send non-work-related e-mails each day, with 32 percent sending between 5 and 10 such messages. Almost 57 percent of employees felt that this personal Internet and e-mail use decreased their productivity.

Yet, despite this widespread activity and acknowledgment that the activity may make them less efficient, only 29 percent of employees

Charles J. Muhl is an attorney with the National Labor Relations Board, Chicago, Illinois. The views expressed in this article are the author's personal views, not an official position of the Board, and represent the author's understanding of the issues and cases discussed. E-mail: charmuhl@sbcglobal.net

reported being caught by their employers engaging in non-work-related Internet surfing. Almost 55 percent of employees thought that their employers were not monitoring either their Internet usage or the e-mails they sent and received. Furthermore, only 57 percent thought that employers should have the right to monitor their employees' Internet and e-mail usage.

Interestingly, employers' viewpoints were largely the same on these questions. More than 82 percent of employers indicated that it was appropriate for employees to view non-work-related Web sites, and 58 percent of these opined that it was permissible for employees to do so between 15 and 30 minutes per day. Similarly, some 86 percent of employers believed that it was appropriate for employees to send personal e-mail, and 61 percent of them felt that one to five messages per day was an appropriate number. Only 31 percent of employers indicated that they monitored or restricted employees' Internet usage, even though 51 percent believed that inappropriate use of the Internet and e-mail compromises worker productivity. The following tabulation presents the main results of the Vault.com survey:

Question	*Percent of employees responding "yes"*	*Percent of employers responding "yes"*
Is it appropriate for employees to surf non-work-related Web sites?	87.5	82.2
Is it appropriate for employees to send personal e-mail during the workday?	83.7	85.8
Have you ever caught an employee (or, if an employee, been caught) in the act of surfing a non-work-related Web site?	28.8	54.0
Does your company monitor or restrict employee Internet or e-mail use (or, if an employee, do you think your employer is monitoring)?	45.5	31.0
Does non-work-related Internet surfing compromise employee activity?	56.6	51.0

Thus, the sentiment among employers and employees alike appears to be that personal Internet and e-mail use at the workplace is fine. But are employers and employees taking legal risks by adopting such a viewpoint? Is an employee's perception that employers do not have the right to monitor Internet and e-mail use supported in the law? Or are employees at risk for being disciplined, including having their jobs terminated, for improper use of the Internet? And what risks do employers assume if they allow employees to use a workplace computer for personal purposes? Can employers be held liable for the behavior of employees who use company e-mail and the Internet?

This article examines how the law has interpreted employers' and employees' rights and risks with respect to Internet and e-mail use at the workplace, beginning with a discussion of whether the law recognizes any right to privacy for employees in the e-mail they send and the Web sites they view at work. The article then examines the risks to employers of permitting employees to use the Internet and e-mail at the office for non-work-related purposes.

Employee risks from personal use

A substantial percentage of employees appears to believe that employers should not have the right to monitor workplace e-mail and Internet use. The law, however, has answered differently to this point. Employees often mistakenly believe that their use of the Internet and e-mail at the workplace is private when, in fact, courts have found no reasonable expectation of privacy in such use and have consistently permitted employers to monitor and review employee activity.

The seminal case in this area is *Smyth* v. *The Pillsbury Company*,[2] originating in the Federal District Court for the Eastern District of Pennsylvania. Plaintiff Michael A. Smyth brought suit against his former employer, The Pillsbury Company, alleging wrongful discharge after the employer terminated him for transmitting what the employer deemed inappropriate and unprofessional comments over the company's e-mail system. Because Smyth was an "at-will" employee, his suit hinged on whether the discharge violated a "public policy" of the State of Pennsylvania and thereby fell into an exception to the general rule that an at-will employee can be terminated at any time for any reason.[3] The court granted the defendant's motion to dismiss the case for failure to state a claim, finding that the employer did not commit the tort of invading the employee's privacy and therefore did not violate public policy in terminating Smyth.

The Pillsbury Company, like many employers, established an e-mail communication system to "promote internal corporate communications between its employees."[4] After establishing the system, the company repeatedly told its employees that all e-mail was confidential and privileged. It also told employees that the company would not intercept their e-mails and then use them as the basis for discipline. In October 1994, Smyth exchanged e-mails with his supervisor over the company's e-mail system. Among other things, the e-mails allegedly contained threats to kill some of the company's sales management staff. The employer intercepted the e-mails and ultimately fired Smyth for making the threats.

Smyth claimed that his termination violated the public policy of Pennsylvania, which he alleged included an employee's right to privacy (in e-mail), as supported in Pennsylvania case law. The plaintiff relied on the tort of "intrusion upon seclusion" in making this argument. That tort is defined in the Restatement (Second) of Torts as follows:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

The court rejected Smyth's contention, finding that there should be no reasonable expectation of privacy in the e-mails sent, despite the company's repeated statements that e-mail would be confidential and privileged. The court noted that Smyth voluntarily communicated with his supervisor over the company e-mail system, which was used by all employees of the company. The court also reasoned that the plaintiff did not disclose any personal information about himself in the e-mails, as would have been the case if the employer had required him to submit to a drug test or a personal-property search. Using a balancing-of-interests test, the court found that, to the extent that Smyth did have a privacy interest in the e-mails, the company's interest in preventing inappropriate and unprofessional behavior outweighed that interest.

That balancing-of-interests test was a common thread in later decisions asserting that an employer's right to maintain a professional and secure workplace outweighs any right to privacy an employee may have in e-mail communications or Internet use. For example, in *United States* v. *Simons*,[5] initially heard before the District Court of the United States for the Eastern District of Virginia, the U.S. Government prosecuted defendant Mark L. Simons, an employee of the Central Intelligence Agency, for violating Federal child pornography laws. The defendant worked in the Foreign Bureau of Information Services division of the Central Intelligence Agency (CIA) and, in that capacity, used the agency's computer system with Internet and e-mail access. During a routine check of the capabilities of the computer system's "firewall," the manager of the computer network noticed a large amount of activity outside the system. Using the keyword "sex," he searched the system's activity logs, believing that such a search would unearth any inappropriate activity. The search returned a significant number of hits that came from the defendant's workstation. Later in the employer's investigation, another information technology professional was told to access the defendant's computer remotely to determine whether any inappropriate pictures or files had been downloaded. The search returned many files that the administrator subsequently classified as pornographic in nature. The administrator then was authorized to copy the defendant's computer hard drive from a remote location. Thereafter, the administrator went into the defendant's office, removed his hard drive, and replaced it with the copy the administrator had made.

Prior to his trial, the defendant moved to suppress the evidence that had been retrieved by the employer. He argued that the searches of his computer were illegal under the fourth amendment to the Constitution, because they were conducted without a warrant or other lawful justification. The court denied the motion, holding that Simons could have no reasonable expectation of privacy in the workplace Internet activity logs and computer hard drive that were searched.

As a preliminary matter, the court reviewed the case law on public-sector employees' reasonable expectation of privacy. The Supreme Court, in *Katz* v. *United States*,[6] enunciated the standard for determining whether employees in the public sector have a right to privacy: a person must have an actual or subjective expectation of privacy, and the expectation must be one that society recognizes as reasonable. (Employees in the private sector are not afforded the protections of the Constitution, including the fourth amendment, in similar situations, because those protections require "State" action, and monitoring by private employers clearly is not a government activity.) For example, in *O'Connor* v. *Ortega*,[7] the Supreme Court held that an employee had a reasonable expectation of privacy in the desk and file cabinets in his or her office. However, the Court indicated that an office's practice or procedures could reduce such an expectation.

In *Simons*, the CIA had an official policy which stipulated that employees could use the Internet for "official business use, incidental use, lawful use, and contractor communications" and that the CIA would conduct electronic auditing of the computer network to "support identification, termination, and prosecution of unauthorized activity," including inbound and outbound file transfers. The Court found that the defendant could not have a reasonable expectation of privacy in his Internet activity, given the CIA's policy. The Court noted further that, even if the defendant had a reasonable expectation of privacy, the Government had a stronger need for supervision, control, and the efficient operation of its workplace. Accordingly, the Government's need would outweigh any right to privacy.

The U.S. Court of Appeals for the Fourth Circuit affirmed the defendant's later conviction and approved the district court's holding with respect to the motion to suppress.[8] Like the district court, the court of appeals found that the employer's Internet policy "placed employees on notice that they could not reasonably expect that their Internet activity would be private."[9] Thus, the employer's review of Internet activity logs and remote searches of the defendant's computer did not violate the fourth amendment, because the defendant could not expect the usage information and the

files on his computer to be private.

The fourth circuit did discuss separately the appropriateness of the employer's removal of the defendant's hard drive from his computer by entering his office. The appellate court did find that, unlike the activity logs and files on the hard drive, Simons' actual office was a place where he had a legitimate expectation of privacy. However, the court permitted the search because it was reasonable in its inception and scope, given the employer's interest in discovering employee misconduct and the prior evidence the employer had of work-related misfeasance by Simons. In particular, the court said that (1) the search was reasonable at its inception because the employer had grounds for suspecting that the hard drive would have evidence of misconduct (the hard drive already had been copied remotely) and (2) the search was permissible in scope because the employer's administrator did nothing more in the office but remove and replace the hard drive. The defendant's desk and other areas of his office were not searched.

The U.S. District Court for the District of Nevada rendered a similar decision in *Bohach* v. *City of Reno*.[10] In this case, two Reno police officers sought a preliminary injunction from the court to halt an internal affairs investigation into text messages the officers sent to each other. The officers claimed that the Reno Police Department's storage of the messages on the department's computer network, as well as the retrieval of the computer files containing the messages, were violations of Federal wiretapping law and of the officers' constitutional right to privacy. Again, because the officers were government employees, the constitutional protections applied to the department's actions.

The department had a software program called Alphapage that permitted officers to transmit brief alphanumeric messages to visual display pagers through the department's local area network. The software program was functionally equivalent to an e-mail system. When the software was implemented, the department had issued a standing order indicating that every Alphapage message was logged onto the network and prohibiting messages that commented on department policy or violated the department's antidiscrimination policy. The messages at issue were alphanumeric and were sent from a computer terminal to a pager.

The court ruled that the officers could not have a reasonable expectation of privacy in their use of the Alphapage system and denied their motion for a preliminary injunction. The court emphasized that the department's standing order reduced employees' expectation that messages would be private. The court also found that, given the type of work in which police officers engage, most officers would expect the department to monitor their communications, whether over a telephone, police radio, or pager.

The *Simons* and *City of Reno* cases illustrate the importance of employers' Internet and e-mail usage policy and the employees' knowledge of, and consent to, that policy. The most certain piece of evidence demonstrating employee awareness and consent to a policy is a signed, written acknowledgment stating that the employee has received, read, and understood the policy. Likewise, although many employees appear to believe that employers do not have the right to monitor their Internet and e-mail usage, in fact employees have no right to privacy in their non-work-related activities, especially when an employer has a clearly articulated policy of which employees are aware.

Like the common law, Federal statutory law also has not afforded employees privacy protection for their personal e-mails or non-work-related Internet use. In 1986, Congress enacted the Electronic Communications Privacy Act to amend the Federal wiretapping laws and afford certain protections to electronic communications. However, the Act does not shield employees when they use the Internet or e-mail at work for personal reasons, because the legislation's protections are directed towards such communications while they are in transit, rather than in storage, and because of certain exceptions that limit the Act's coverage.

The Electronic Communications Privacy Act, along with other prohibitions, restricts the intentional interception of an "electronic communication," defined to include e-mail.[11] "Interception" implies access to the e-mail while it is in transit. Access to e-mail stored on a computer server is arguably outside the scope of the Act's protections. (The *City of Reno* court, for example, noted that the e-mail messages at issue were retrieved from storage, not during their actual transmission.)

Further, the ban on e-mail interception is limited by three different exceptions, any one of which may permit an employer to monitor employees' e-mail usage. The *consent exception*[12] permits a party to monitor the e-mail use of individuals who previously have consented to monitoring, such as when an employer provides a policy on use that the employee acknowledges having read. The *provider exception*[13] allows a provider of e-mail services to intercept e-mails on its system, meaning that employers are not forbidden from examining e-mail on systems they furnish to their employees. Arguably, the employees' system must be provided by an employer and not a third-party servicer. The *ordinary-course-of-business exception*[14] permits a party to monitor e-mail messages sent as part of the ordinary course of business. Although this exception literally applies only to work-related e-mails, the exception might permit an employer to access personal e-mails when they are sent on a business system.

Thus, like the common law, Federal statutes do not protect employees' personal use of the Internet or e-mail at the workplace. Employees who feel that such activity is private and should not be monitored by employers are mistaken under the law.

Employer risks from failure to monitor

The law permits employers to monitor employees' Internet and e-mail use, especially when the employees have consented to such monitoring. Yet, in the survey results described in the introductory section of this article, fewer than one-third of employers indicated that they actively monitor employees' Internet activity. What risks are employers running by not monitoring such activity? The short answer is "many."

Because computer networks can store incoming and outgoing messages, parties to lawsuits increasingly submit e-mail as evidence when they seek to hold an employer liable for claims such as defamation, sexual harassment, racial or ethnic discrimination, and copyright or trademark infringement.[15] However, the employee-plaintiffs in these cases succeed only infrequently.

Defamation. In *Meloff* v. *The New York Life Insurance Company*,[16] initially heard before the District Court of the United States for the Southern District of New York, plaintiff Phyllis Meloff brought a claim of retaliation based in part upon her employer's defamation of her. She had worked almost three decades with New York Life when she was fired from her position as a service consultant, allegedly for misuse of her corporate credit card.

The evidence at trial showed that Meloff had violated company policy by using her corporate credit card to charge personal expenses for which she never reimbursed the employer. She met a number of times with her supervisors, including James Mellbye, and ultimately was terminated. Immediately following the meeting that culminated in her termination, Mellbye sent an e-mail to seven persons which had the subject title "FRAUD" and which stated,

> WE FOUND IT NECESSARY TODAY TO TERMINATE PHYLLIS MELOFF, WHO USED HER CORPORATE AMERICAN EXPRESS CARD IN A WAY IN WHICH THE COMPANY WAS DEFRAUDED. PHYLISS [SIC] HAD APPROX [SIC] 27 YEARS WITH NEW YORK LIFE, AND WHOM [SIC] WE CONSIDERED TO BE A VALUED ASSOCIATE. THIS ACTION REFLECTS OUR COMMITTMENT [SIC] TO "ADHERE TO THE HIGHEST ETHICAL STANDARDS IN ALL OUR BUSINESS DEALINGS." I SEND THIS TO YOU FOR YOUR OWN INFORMATION.

Five of the seven people who originally received the e-mail were officers of the company who had subordinates trained by Meloff. The e-mail was later forwarded to four other managers who worked on a specific project with Meloff and to five other employees who had worked with her at various times. Following a trial, a jury awarded Meloff $250,000 in compensatory damages and $1,000,000 in punitive damages on the defamation claim.

However, following the trial, the district court granted the employer's motion for judgment as a matter of law (thereby effectively throwing out the jury's verdict), holding that there was no evidence from which the jury could have found that the employer "abused its qualified privilege" in making the defamatory statement. Pursuant to New York law under which the suit was brought, a party can defend a defamation action by arguing that the statement was protected by a qualified privilege. The privilege extends to statements made in the employment context concerning the qualifications and actions of employees, where the statements are made by a person with an interest in commenting, or duty to comment, on an employee and to a person with a common interest in the statements' subject matter. Even when a statement is protected by the privilege, though, an employer can abuse the privilege and be subject to liability if the statement is shown to be false and published (1) with the knowledge that it was false or with a reckless disregard for its truth, (2) with common-law malice, or (3) outside the scope of the privilege. Although it held that the trial record may have supported the jury's finding that the statement was defamatory, the district court ruled that no evidence was submitted by the plaintiff which tended to show that the employer distributed the e-mail in bad faith.

The Second Circuit Court of Appeals overturned the district court's granting of judgment as a matter of law to the defendant.[17] The appeals court relied heavily on precedent granting no leeway to a trial judge to substitute a personal opinion for the jury's verdict on the evidence presented. The court first stated that there was no reason for the trial judge to overturn the jury's finding that the accusation, "FRAUD," in the e-mail's title was not substantially true, because the jury was qualified to determine what the impression of the word "fraud" would be on an average listener. Furthermore, the court upheld the jury's finding that the employer acted with malice in sending the e-mail and thereby abused its qualified privilege, because Mellbye had assured Meloff, after the credit card abuse was initially discovered, that it was "no problem," but less than a week later sent the inflammatory e-mail. Accordingly, a new trial was ordered for the case.

Lian v. *Sedgwick James of New York, Inc.*,[18] involved a similar defamation action brought in the Southern District of New York. Plaintiff Philip Lian alleged that he was defamed by his employer when his supervisor sent an e-mail to other members of his department which stated that Lian had agreed to begin looking for other employment. Lian worked as an insurance salesperson and had a difficult relationship with his supervisor, Brian Innes. In particular, Innes felt that Lian failed to adhere to company procedure in his handling of certain insurance sale transactions and client matters. In the insurance industry, an agent can be subject to "errors and omissions" (E&O) liability for negligent acts or omissions in professional conduct. In a meeting between Lian and Innes, Lian allegedly told Innes that he wanted to continue working

for Sedgwick through the end of 1996. Subsequently, Innes sent the following e-mail to four otheremployees who held managerial positions with the company:

> I have today agreed with Phil Lian that he will begin to seek employment and opportunity outside of Sedgwick effective immediately. We have agreed that he may remain on the payroll 60 days (including, not in addition to, any accrued vacation time) to effect this transition and to use his office on the 3rd floor only to arrange interviews, etc.
>
> Phil had agreed he is NOT to transact any further business in the name of Sedgwick. We have agreed to assist in the transition of business he has generated to his new employer, i.e. we will honor Letters of Appointment he may produce. These measures are necessary to protect our E&O exposure.
>
> We both hope the process will not take 60 days but have also agreed it will not take longer as far as Sedgwick is concerned—the end of June is the closure date we have agreed [on].
>
> Please effect the necessary measures from a personnel and security perspective and let me know if you have any questions. Thank you.

The plaintiff contended that the information in the e-mail was false and that he had never agreed with Innes that he would seek employment somewhere else. He further alleged that the dissemination of the e-mail caused him so much embarrassment that he was forced to resign shortly thereafter.

The court granted the employer's motion for summary judgment on the claim, finding that the content of the e-mail was not defamatory. The plaintiff's argument essentially was that the e-mail suggested that he was forced to resign from Sedgwick because he had exposed Sedgwick to potential E&O liability through his professional negligence or malpractice. Under New York State law, in order to sustain a defamation claim, a plaintiff is required to show that a party wrongfully published, to third persons, a false or defamatory statement about the plaintiff that injured the plaintiff's reputation. In this case, Lian argued that the statement was libelous "per se" (meaning that he did not have to prove special damages—specific instances in which he lost money as a result of the statement), because it disparaged him in his office, profession, or trade.

The court analyzed whether the e-mail was subject to more than one interpretation. As required by New York law, when a court finds that a statement is capable of only one interpretation, it then determines whether that interpretation is defamatory. In Lian, the court found that the e-mail consisted merely of (1) an announcement that the plaintiff's employment with Sedgwick would be ending and (2) instructions to other personnel to take the necessary measures that accompany such an end of employment. The court noted that the mere assertion of a person's discharge or termination from employment is not defamatory, even if it is untrue, except when the statement implies that the termination was a result of employee misconduct. Because the e-mail suggested that the parties mutually agreed to end Lian's employment, the court found no implication of misconduct. Therefore, the court granted judgment to the employer.

Employers do risk liability for defamation when their supervisors, managers, or other employees send e-mails to other workers concerning the performance of an employee. This risk is exacerbated by the ease with which e-mails can be distributed and the often inflammatory contents of messages sent in the aftermath of emotional events at the workplace.

Sexual harassment. Evidence to support sexual harassment claims has increasingly come in the form of printed e-mail messages between employees. However, the messages alone are often insufficient to sustain a plaintiff's cause of action.

In *Schwenn* v. *Anheuser-Busch, Inc.*,[19] plaintiff Deborah Schwenn brought a sexual harassment complaint in the District Court of the United States for the Northern District of New York against her employer under New York State law. The case was based principally upon alleged sexually harassing e-mail messages she received on the computer terminal attached to the forklift trucks she operated in the local Anheuser-Busch warehouse. Schwenn made a complaint to her supervisors, who then conducted meetings with all of the company's workers. At those meetings, the company reiterated the employer's policy against sexual harassment and notified the workers that the employer would audit e-mail messages to ensure compliance with the policy. Schwenn worked two more shifts at the warehouse after the meetings. She claimed that, during those shifts, her coworkers retaliated against her for complaining about the e-mails. After the plaintiff temporarily left work, the employer printed and reviewed all e-mail messages residing on the warehouse computers, but could not locate any offensive ones.

Anheuser-Busch moved for summary judgment on the plaintiff's complaint, contending that the injuries alleged by Schwenn—principally the receipt of the e-mails—were insufficient to sustain a sexual harassment complaint premised on a hostile work environment.[20] The district court granted the defendant's motion. The court compared the alleged 3-week period of harassment and the receipt of e-mail messages with other cases in which a hostile work environment was found, after which it reasoned that Schwenn's work environment was not significantly altered by the e-mail messages or other behavior of her coworkers.

Similarly, in *Rudas* v. *Nationwide Mutual Insurance Company*,[21] the District Court of the United States for the

Eastern District of Pennsylvania granted the defendant's motion for summary judgment on the plaintiff's retaliation claim under the Pennsylvania Human Relations Act. The court found that, although the plaintiff produced evidence of sexual harassment—including several sexually explicit e-mails sent by her former supervisor—the employer had not taken any retaliatory action against her for lodging a formal sexual harassment complaint.

Even though employers have been successful with motions for summary judgment and motions to dismiss complaints for sexual harassment premised in part on e-mail evidence, that evidence can be sufficient to sustain a plaintiff's case under certain circumstances. In *Knox* v. *State of Indiana*,[22] for example, the Seventh Circuit Court of Appeals affirmed a jury's verdict in favor of an employee on her claim, brought under Title VII of the 1964 Civil Rights Act, of employer retaliation in response to a sexual harassment charge she lodged. Plaintiff Kristi Knox worked as a correctional officer at the Correctional Industrial Complex in Pendleton, Indiana. During her employment, her supervisor, Robert Stewart, sent her e-mails in which he propositioned the plaintiff by using acronyms such as "HGTWM," which translated into "horizontal good time with me." Stewart also left her phone messages reminding her to check her e-mail. Knox consistently rebuffed Stewart, ultimately leading him to comment that he "definitely saw a shift change in [her] future."[23] She then filed a formal complaint with the company regarding Stewart's behavior. Initially, he denied any knowledge of why Knox would file a complaint against him, but the employer confronted him with copies of the e-mails he had sent. Thereafter, Stewart acknowledged that his behavior could have appeared sexually harassing. During the employer's investigation, Stewart's friends on the job told Knox that they were going to make her life "hell" and that they were going to "get her." The appeals court found that the evidence could support the jury's finding that Knox had made an appropriate complaint to her employer and had been retaliated against because of the complaint.

E-mail evidence alone likely will not result in employer liability for sexual harassment, especially when an employer has a mechanism for employees to report such complaints and takes remedial action after learning of the complaint. However, inappropriate e-mail activity, coupled with other failures on the employer's part, can result in liability. Furthermore, the foregoing cases demonstrate that at least some employees fail to realize that the inappropriate messages they send to their coworkers may not be viewed solely by the recipients in the "To:" list of the e-mail.

Racial discrimination. Much as in the sexual harassment cases just described, plaintiffs also have supported claims of racial discrimination through the introduction of e-mail evidence. In *Copley* v. *Bax Global*,[24] heard before the District Court of the United States for the Southern District of Florida, a former employee sued his employer under the Federal civil rights law prohibiting racial discrimination in the formation of contracts.[25] The plaintiff claimed that he was fired from his job because he was not Hispanic. Lester Copley, a white man, was manager of Bax Global's Ocean Services division for Florida and Latin America, from which the company conducted international shipping. His job involved moving freight through the company's Miami station. The plaintiff did not have an employment contract and, accordingly, was an at-will employee. Over a period of 2 years, the company's president received a number of complaints from Latin American agents concerning Copley's job performance. As a result, the plaintiff was terminated. Almost immediately, he was replaced by Mariano Rabayo, a Canadian citizen who was born in Bogotá, Colombia.

Plaintiffs can prove a prima facie case of racial discrimination under Federal civil rights law by using direct, circumstantial, or statistical evidence. In this case, the plaintiff relied chiefly on e-mail messages to substantiate his claim, arguing that the messages were both direct and circumstantial evidence that he was fired because he was white. The e-mail messages focused on Copley's termination and included (1) discussions about what action should be taken against him (transfer or termination) as a result of the complaints, (2) a statement that Copley's removal would inspire confidence in the company's Latin American agents, and (3) concerns about the appearance of naming Rabayo as Copley's replacement only a day after Copley would be terminated. However, none of the messages was clear about the company's reason for terminating Copley.

The district court denied the employer's motion for summary judgment in the case, finding that the e-mail messages and other statements attributed to the employer were circumstantial evidence of racial discrimination. Because the e-mail messages made no direct reference to the employer's motivation in firing Copley, the court found that they did not constitute direct evidence of racial discrimination. However, the e-mail messages and a statement attributed to the plaintiff's supervisor asserting that he "didn't think that a blue-eyed blond-haired fellow would ever get along well in Latin America and that we needed a Latin manager of the office to achieve any level of success" were together sufficient to support an inference that the employer was motivated by Copley's race in deciding to terminate him. That inference cast doubt on the employer's stated reason for the firing—complaints from the Latin American agents—meaning that the issue of whether the reason was a pretext for the firing was a question of fact for a jury to resolve at trial, not for the court to decide by means of a summary judgment motion.

A number of different courts have ruled in favor of employers in cases where racial discrimination claims are based

solely on a small number of e-mail messages. For example, in *Harley* v. *McCoach*,[26] the Federal District Court for the Eastern District of Pennsylvania granted the employer's motion for summary judgment on a racial discrimination claim, finding that a lone e-mail referring to the plaintiff as "Brown Sugar," an alleged incident in which the plaintiff's boss referred to her with the "n" word, and her coworkers' reference to her being the Whitney Houston character from the movie *The Bodyguard* because of an alleged affair with her boss were insufficient to show a hostile work environment. Similarly, in *Owens* v. *Morgan Stanley & Co., Inc.*,[27] the Federal District Court for the Southern District of New York granted the employer's motion to dismiss a racially hostile work environment claim, finding that one e-mail containing racist jokes, while reprehensible, was insufficient to support the claim. Finally, in *Daniels* v. *Worldcom Corp.*,[28] the District Court of the United States for the Northern District of Texas granted the employer's motion for summary judgment on the plaintiff's complaint that the employer negligently permitted employees to use the company's e-mail system to send racially discriminatory jokes. The court was persuaded by the employer's prompt remedial action after being advised of the four e-mails, including reprimanding the employees who sent them and advising all employees of the company's policy on Internet and e-mail use.

These cases make clear that certain racial discrimination complaints can go to trial on the basis of substantial e-mail evidence, but that claims premised on infrequent occurrences are not likely to succeed. Again, employers face less risk when they implement a policy regarding Internet and e-mail use.

Copyrights and trademarks. Theoretically, employers could be held liable for employees' violations of another party's copyrights or trademarks in situations where the violation occurs as part of the employee's normal business. In the context of Internet use and e-mail, the most obvious potential violation is an employee's downloading of files from the Internet that have copyright or trademark protections and then using those files to further the business of the employer in some manner.[29]

In sum, employers run risks from failing to monitor employees' Internet and e-mail use. Plaintiffs have brought and supported many kinds of cases against employers, based in whole or in part on e-mail evidence. Few of the reported cases, however, have resulted in success for those plaintiffs. Nonetheless, employers bear substantial litigation costs in defending such suits; even taking a case to summary judgment, with the necessary depositions of witnesses and preparation of the motion and briefs, can run into tens of thousands of dollars, to say nothing of proceeding to trial. That danger should motivate employers to implement clear and detailed policies on the appropriate use of e-mail by employees, as well as to monitor e-mail use to ensure that employees are complying with the policy.

Employer policies

What should an employer's policy on Internet and e-mail use articulate? The answer depends on the particular uses and restrictions the employer decides to implement, but some general guidelines apply to all situations. Employers should delineate what are and what are not permissible uses of the Internet and e-mail at the workplace and should clearly detail what personal use of those services will be allowed, if any. Of course, employers should inform employees that any discriminatory or other illegal use of the Internet or e-mail is prohibited. Employers also should state that employees' use of the employer's e-mail system and Internet access is neither confidential nor private. Employers should monitor employees' use and should state in the policy that such monitoring will occur.

Are any dangers posed to employers from implementing such a policy? At least one has arisen in the context of employers whose employees are conducting a union-organizing campaign. The National Labor Relations Act grants employees the right, among other things, to organize and to engage in protected concerted activities. Under the National Labor Relations Board's decision in *E. I. DuPont de Nemours & Co.*,[30] an employer cannot allow employees to use a business e-mail system to discuss personal topics, but at the same time forbid them from discussing whether to join a union. Where employers permit personal use, employees are free to distribute union literature through e-mail. The Board also held, in *Timekeeping Systems, Inc.*,[31] that an employer cannot discharge or otherwise discipline an employee for sending an e-mail to other employees with commentary on a proposed change in benefits that the employer is contemplating or intending to implement. Such activity is concerted and protected.

The cases of *DuPont* and *Timkeeping Systems* suggest that an employer should not prohibit employees' discussions of organizing or working conditions when the employer permits other personal use of e-mail or the Internet.[32] In addition, the General Counsel's office (the investigatory and prosecutorial wing of the Labor Board) previously indicated that it considers an employer's rule prohibiting all non-business use of e-mail as invalid under Board case-law precedent interpreting the National Labor Relations Act. However, no official Board decision has yet been reached on this issue.[33]

A commonsense approach

Both employers and employees agree that non-work-related use

Exhibit 1. Employer and employee myths and legal realities regarding Internet and e-mail use in the workplace

Myth	Legal reality
My employer does not have the right to read my personal e-mail or review the Internet sites I visited.	Employees have no privacy rights in their e-mail and Internet use, and Federal law does not prohibit employers from monitoring that use.
It is no big deal if my employees use e-mail or the Internet for personal reasons on the job. As an employer, I do not need to monitor their use.	Failure to monitor employees' e-mail and Internet use can lead to legal liability in more ways than one.
If I, as an employer, am facing legal liability for employees' e-mail and Internet use, I should just prohibit them from any personal use.	Employers may be violating Federal labor law by implementing blanket prohibitions on personal use.

of the Internet and e-mail is appropriate, and indeed, many employees now see such activity as essential to "making it through" the workday. As with most things in life, a commonsense approach to this issue minimizes the risks for all involved: employees must acknowledge that their employers can and will monitor their use of these two electronic means of communication to ensure that it is not excessive, inappropriate, or illegal, and employers must make all employees aware of their policies and procedures with respect to the Internet and e-mail, reviewing employee activity or quickly taking remedial action when those policies or procedures are violated. Exhibit 1 presents the chief myths and the corresponding legal realities regarding the use of e-mails and the Internet in the workplace. □

Notes

[1] In September 1999, Vault.com, a Web site devoted to assisting people with a job search or building a career, "surveyed 1,244 employees and 1,438 employers to determine how Web surfing and e-mail use affect productivity and quality of life at work" (See Vault.com Web site.) The survey addressed employees' Internet and e-mail use at work, employers' monitoring of that use, and the effect that such use had on employees' productivity. See **http://www.vault.com/surveys/internetuse/internetuse.jsp**, last visited Dec. 17, 2002.

[2] 914 F. Supp. 97 (E.D. Penn. 1996).

[3] For a detailed discussion of the employment-at-will doctrine and exceptions to the general rule, see Charles J. Muhl, "The employment-at-will doctrine: three major exceptions," *Monthly Labor Review*, January 2001, pp. 3–11.

[4] 914 F. Supp. at 98.

[5] 29 F. Supp. 324 (E.D. Va. 1998).

[6] 389 U.S. 347, 361 (1967).

[7] 480 U.S. 709, 717–18 (1987).

[8] *United States* v. *Simons*, 206 F.3d 392 (4th Cir. 2000).

[9] 206 F.3d at 398.

[10] 932 F. Supp. 1232 (D. Nev. 1996).

[11] 18 U.S.C. 2510 and 2511(1).

[12] 18 U.S.C. 2511(2)(d).

[13] 18 U.S.C. 2510(5)(a)(ii).

[14] 18 U.S.C. 2511(2)(a)(i).

[15] Generally, an employer cannot be held liable for an employee's conduct, unless the employee is acting within the course and scope of employment.

[16] 1999 WL 604871 (S.D. N.Y. 1999).

[17] *Meloff* v. *The New York Life Insurance Company*, 240 F.3d 138 (2nd Cir. 2001).

[18] 992 F. Supp. 644 (S.D. N.Y. 1998).

[19] 1998 WL 166845 (N.D. N.Y. 1998).

[20] For a more detailed discussion of the various types of sexual harassment claims and the standards used by courts to evaluate them, see Charles J. Muhl, "The Law at Work: Sexual Harassment," *Monthly Labor Review*, July 1998, pp. 61–62.

[21] 1997 WL 634501 (E.D. Pa. 1997).

[22] 93 F.3d 1327 (7th Cir. 1996).

[23] 93 F. 3d at 1330.

[24] 80 F.Supp.2d 1342 (S.D. Fla. 2000).

[25] 42 U.S.C. 1981 provides, in part, that "All persons within the jurisdiction of the United States shall have the same right in every State and Territory to make and enforce contracts...as white citizen[s]." Although courts have disagreed as to whether an at-will employee can bring a claim under Section 1981 (because at-will employees do not have a formal employment contract), the district court here found such a claim to be actionable. (See *Copley,* 80 F.Supp.2d at 1345–48.)

[26] 928 F. Supp. 533 (E.D. Pa. 1996).

[27] 1997 WL 403454 (S.D.N.Y. 1997).

[28] 1998 WL 91261 (N.D. Tex. 1998).

[29] To my knowledge, no reported cases exist in which such a theory of liability has been advanced. For a general discussion of potential copyright violations resulting from the posting of copyrighted works on the Internet, see *Marobie-FL, Inc.*, v. *National Association of Fire Equipment Distributors and Northwest Nexus, Inc.*, 983 F. Supp. 1167 (N.D. Ill. 1997).

[30] 311 NLRB 893 (1993).

[31] 323 NLRB 244 (1997).

[32] For a more thorough discussion of the issues that e-mail and the Internet create with respect to the National Labor Relations Act, see Michael Josserand, "The Impact of Employer Rules That Limit E-mail Use and Internet Access," *Colorado Lawyer*, October 2000, pp. 7–11.

[33] In *The Guard Publishing Company*, Case Number 36-CA-8743–1 et al., an administrative law judge rejected the General Counsel's position and held that the National Labor Relations Act does not prohibit an employer's policy that limits e-mail use to business purposes, so long as the policy is applied neutrally. In a neutral application, the employer cannot permit certain personal uses, but then forbid discussion of union organizing or other union activities. This decision came at the trial stage of a case brought by the General Counsel's office against an employer. The Board may have the opportunity to rule on the issue in the near future if exceptions (appeals) to the administrative law judge's decision on the question are filed by any party to the case.