

Communications Technology in the Workplace

Jeffrey M. Place
Spencer Fane Britt & Browne LLP
1000 Walnut St., Suite 1400
Kansas City, Missouri 64106-2140
(816) 474-8100 (telephone)
(816) 474-3216 (facsimile)

I. E-Mail.

A. Risks Arising from Employee Use of E-Mail and the Need to Monitor.

1. Workplace Harassment.

Under Title VII and Section 1981, employers are obligated to make reasonable efforts to prevent harassment based on race, gender and other protected categories, and they must take prompt and effective remedial action to eliminate any harassment that exists. These obligations clearly create a need to monitor employee use of e-mail systems.

Harassment claims based in whole or in part on e-mail messages are becoming more common as e-mail use continues to explode. While courts recognize the potential for e-mail to be used as a tool of harassment, they have also refused to find that every offensive or inappropriate message creates a cause of action. For example, in *Curtis v. Dimaio*, 46 F. Supp. 2d 206 (E.D.N.Y. 1999), two Citibank employees asserted Section 1981 claims alleging racial harassment based on an e-mail joke about *Æbonics*.[®] The court dismissed the claim, noting that the single joke was not severe enough to support a cause of action, especially because it was not sent to the plaintiffs. *See also Owens v. Morgan Stanley & Co.*, 74 F.E.P. Cases 876 (S.D.N.Y. 1997) (e-mail containing racist joke and circulated among white employees not sufficient to support hostile work environment claim; *A*instead of sporadic racial slurs, there must be a steady barrage of opprobrious racial comments[®]).

Similarly, in *Schwenn v. Anheuser-Busch, Inc.*, 1998 WL 166845 (N.D.N.Y. 1998), the court granted summary judgment on a claim of sexual harassment, finding that

several messages received on a computer terminal attached to the plaintiff's forklift were not sufficiently severe to create a hostile work environment. *See also Baer v. Sprint Long Distance*, 60 F. Supp. 2d 209 (S.D.N.Y. 1999) (single pornographic picture e-mailed to plaintiff's work computer by co-worker does not create a sexually hostile work environment).

Despite these favorable decisions, employers must remain especially sensitive to inappropriate use of e-mail or Internet resources in the workplace. Because these technologies create permanent or semi-permanent records of inappropriate activity, they can be especially strong evidence of management complicity or negligence in permitting or fostering a hostile environment.

2. Lost Time.

Lost time due to personal e-mail or Internet use is a serious problem for many employers. In a study conducted during the last quarter of 1997, managers at Chevron were surprised to find that 46% of all employee Internet use was for non-business purposes, and 5% of all use was dedicated to downloading sexually explicit material. Mary Curtius, *Technology: A Love-Hate Relationship* **C***Surf Warning Your Employer Has A Legal Right to Monitor Your Computer Activity at the Office*, L.A. TIMES, January 19, 1998. In one recent survey, half of all responding employees admitted to spending more than thirty minutes per day on non-work related Internet use and responding to personal e-mail. Fifty-six percent admitted that Internet and external e-mail access made them less productive at work. Diane Stafford, *Surfing the Net on the Clock*, KANSAS CITY STAR, December 11, 1999. With numbers like these, many employers may conclude that they cannot afford not to place some reasonable limits on personal computer use at work, and must take steps to enforce those limits.

3. Information Theft.

Two types of information theft should concern employers when considering employee e-mail use. First, external e-mail offers a simple route for employees to remove trade secret or confidential information from the workplace. An employee may not even need to leave his or her work station to access key documents and send them outside of the company as attachments to an e-mail message. Such activity may be malicious, directing important information to a competitor, or it may be as benign as a well meaning employee e-mailing documents to his or her personal e-mail address to work on them at home. Either way, the ability to send sensitive information outside of the company creates substantial risks to a company's information assets. Thus, employers

with especially valuable trade secret or confidential data, ranging from technical diagrams to customer and price lists, have a strong incentive to monitor employee e-mail use.

The second type of information misuse employers must consider when employees have e-mail or Internet access is copyright violation. Cases involving suits for Internet-related copyright violations have ballooned in recent years, and include disputes involving posting of documents ranging from photographs scanned from Playboy magazine to copies of religious texts. A huge volume of copyrighted information is available on the Internet, and if an employee misappropriates that information over a company computer and the company reaps a financial benefit (with or without specific knowledge of the violation), the company may be vicariously liable for the employee's copyright violation. If the company learns of the employee's violation and is in a position to end the employee's use of the copyrighted material, but fails to do so, the company may be liable for contributory infringement of the copyright. For more on this topic, see THOMAS P. KLEIN, *ELECTRONIC COMMUNICATIONS IN THE WORKPLACE: LEGAL ISSUES AND POLICIES*, 563 PLI/Pat 695 (1999).

4. Defamation.

The permanent, written nature of e-mail, together with the ability to send copies of messages to numerous recipients or forward received messages creates a clear exposure to claims of libel. Generally, a plaintiff may establish a claim for libel by showing that the defendant wrongfully published to a third person a false and defamatory statement of and concerning the plaintiff, and that the statement injured the plaintiff's reputation.

In *Lian v. Sedgwick James of New York*, 992 F. Supp. 2d 644 (S.D.N.Y. 1998), a manager sent an e-mail message to the plaintiff's co-workers informing them that he had reached an agreement with the plaintiff, and the plaintiff would begin looking for work elsewhere. Within a few minutes, the manager copied and forwarded the message to a number of company employees, with various comments added. Plaintiff asserted that he had never agreed to leave the company, but was forced to resign after the message was distributed because it falsely implied that he was incompetent. Reviewing the wording of the message, the court concluded that it did not imply incompetence, but merely stated that the parties had mutually agreed that plaintiff would seek other employment. The court noted, however, that statements that do in fact disparage a person in his or her trade, or that insinuate that a person has committed a crime, are libelous per se.

In another defamation case involving e-mail use, Beekmans, a Norwegian banker met for dinner with a J.P. Morgan employee in London. *Beekmans v. J.P. Morgan & Co.*, 945 F. Supp. 90 (S.D.N.Y. 1996). Following the dinner, the J.P. Morgan employee sent an e-mail to six other members of the firm stating that Beekmans had made statements that were potentially damaging to his employer, appeared intoxicated, and had made racially inflammatory comments. The message was subsequently forwarded to others elsewhere, and J.P. Morgan employees in New York ultimately decided to disclose the message to Beekman's employer. Beekman was discharged, and filed suit for defamation. The claim was dismissed on forum non conveniens grounds, because most of the key witnesses lived in Norway. However, these facts clearly illustrate the way in which e-mail can contribute to defamation claims.

Clearly, e-mail messages explaining the reasons for disciplinary decisions could easily result in liability for defamation. If such messages are absolutely necessary, they should be distributed as narrowly as possible, preferably by some means other than e-mail so that they will not be forwarded.

5. Damage to Company Image or Name.

E-mail also poses a potential threat to a company's goodwill. Many e-mail headers or automatic signatures identify not only the sender of a message, but the company for which he or she works, where the message originated. While harassment problems are a concern when employees receive questionable messages, companies may be equally concerned about seeing their corporate name or logo on a racially offensive or sexist joke sent to friends by one of their own employees. Again, the widespread popularity of forwarded messages may in some cases lead to rapid distribution of employee comments to a network of people across the country and around the world, most of whom have never met the author of the message.

6. Discoverable Evidence in Litigation.

In *Strauss v. Microsoft Corp.*, 814 F. Supp. 1186 (S.D.N.Y. 1993), the plaintiff claimed that defendant had failed to promote her to the position of technical editor of defendant's trade magazine because of her gender, and had instead hired a less-qualified male for the position. The court denied defendant's motion for summary judgment, finding that a reasonable jury could conclude that plaintiff was more qualified than the hired male, and that gender was a factor in defendant's decision making. The court's ruling was based in part on an e-mail message in which a higher-level executive warned the decision maker that the person actually promoted will

have one heck of a learning curve to come up on since he has not even written for publication, much less acquired materials or managed the editorial process . . . IF you decide he is your candidate, then he needs . . . a real, real strong right hand person . . . involved in TRAINING him on the issues and problems.@ Additionally, the court noted that an e-mail from the decision maker to subordinates contained sexual innuendo in the form of a reference to Amouse balls,@ and found that this type of language in the workplace contributed to an inference of gender-based decision making.

Of course, not every e-mail message will be automatically admissible in every case. In *Monotype Corp. v. International Typeface Corp.*, 43 F.3d 443 (9th Cir. 1994), the court excluded an e-mail message that contained Aa highly derogatory and offensive description@ of plaintiff's type director, holding that the message was unfairly prejudicial to the defendant under Federal Rule of Evidence 403. The court additionally noted that e-mail is A less of a systematic business activity@ than certain other types of computerized records, and thus more easily subject to exclusion.

B. Attacks Employees Commonly Make On Monitoring Policies.

1. Constitutional Claims.

For public employers, e-mail monitoring policies may raise Fourth Amendment concerns. In *O'Connor v. Ortega*, 480 U.S. 709, 107 S. Ct. 1492 (1987), a public employer conducted a search of an employee's office, desk and file cabinets as part of an investigation into possible sexual harassment and improper financial dealings. The employee challenged the search under the Fourth Amendment. The Supreme Court held that whether the Fourth Amendment had been violated depended first upon whether the employee had a reasonable expectation of privacy in his office, and second upon whether, balancing the employee's privacy expectations against the employer's motivations for the search, the search was reasonable in its inception and scope. Whether an employee has a reasonable expectation of privacy will depend upon the actual operation of the workplace, together with its policies and procedures. If a reasonable expectation exists, the search must then be evaluated for reasonableness of inception and scope based on all the circumstances of the case.

Under the *O'Connor* analysis, if a public employer takes steps that create a reasonable expectation of privacy in the employee's e-mail messages, its

searches will be subject to review for reasonableness under the particular circumstances of the case.

2. Federal Wiretapping Claims.

The Federal Wiretap Act, 18 U.S.C. ' ' 2510-2522 prohibits the interception of oral, wire and electronic communications. This statute is key to the analysis of telephone monitoring or tape recording of oral conversations. However, it normally will not apply to e-mail or voice mail, because such communications are not typically intercepted, but are instead accessed in a stored format on a computer after they have been sent or received.

In *Wesley College v. Pitts*, 974 F. Supp. 375 (D. Del. 1997), the court found that a college employee did not violate the Federal Wiretap Act when he inadvertently saw an e-mail message on a computer screen, and then conveyed the contents of the message to other employees, because viewing the message on a computer screen did not amount to interception.

The Electronic Communications Privacy Act, 18 U.S.C. ' ' 2701-2711, an amendment to the Wiretap Act, prohibits the unauthorized access, use or disclosure of stored communications. However, it includes an exception for system providers. Thus, employers will not normally violate this statute by accessing e-mail messages stored on their own computers. It is unclear whether an employer who hires a third-party provider for external e-mail service would violate the act by accessing e-mail stored on the third-party's computer systems.

2. State Wiretapping Claims.

State statutes generally track the Federal Wiretap Act, prohibiting interception of e-mail messages, but not the act of accessing those messages once stored as a computer record. *See, e.g.*, FLA. ST. ANN. ' 934.03.

Connecticut has passed a statute requiring employers to post a notice to employees describing any electronic monitoring that may occur in the workplace. Electronic monitoring is defined very broadly to cover the collection of information about employee activity by any means other than direct observation. *See* St. St. ' 31-48d. Other state legislatures have considered legislation to extend privacy protections to cover employee e-mail messages. *See* Section I.C., below.

3. Invasion of Privacy Claims (the Problem with Passwords).

The common law tort for intrusion upon seclusion prohibits a person or entity from intruding physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, where the intrusion would be highly offensive to a reasonable person. Restatement (Second) of Torts ' 652B. Employees may claim that an employer commits this tort by accessing an employee's personal e-mail communications initiated from the workplace.

When courts consider whether an intrusion would be highly offensive to a reasonable person, they first consider whether the plaintiff had a reasonable expectation of privacy. Many commentators and a few courts have reasoned that individual passwords or other indicators of privacy could create an expectation in employees that their employer will not view their e-mail.

However, most courts have rejected this sort of claim. In *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996), the employer told its employees that their communications over its e-mail system would be confidential, and could not be used as grounds for termination or reprimand. Plaintiff, a regional operations manager, sent an e-mail to his supervisor complaining about sales management in which he threatened to kill the backstabbing bastards, and referring to a holiday party as the Jim Jones Koolaid affair. He was then discharged, and sued for invasion of privacy. The court dismissed plaintiff's complaint for failure to state a claim upon which relief could be granted, holding that employees have no reasonable expectation of privacy in e-mail communications sent over the employer's system, irrespective of company assurances to the contrary. Furthermore, the court found that the company's interest in preventing inappropriate or unprofessional communication outweighed any privacy interest employees might have in their e-mail communications, and any intrusion thus would not be offensive to a reasonable person.

By way of comparison, note that courts have been more solicitous towards claims that other types of communication in the workplace should remain private. In *Ali v. Douglas Cable Communications, Inc.*, 929 F. Supp. 1362 (D. Kan. 1996), the court held that indiscriminate recording of all telephone conversations without first warning employees may constitute actionable invasion of privacy (intrusion upon seclusion). The court concluded that a reasonable person might find this activity highly offensive.

In *McLaren v. Microsoft Corp.*, 1999 WL 339015 (Tex. App. 1999), the plaintiff asserted that his employer invaded his privacy by accessing e-mail messages stored in his personal folders in his office computer during a sexual harassment investigation. The company permitted its employees to establish personal passwords to restrict access to personal folders, and plaintiff asserted that this established a reasonable expectation of privacy. The court concluded that plaintiff had no reasonable expectation of privacy in his personal folders, notwithstanding the password, because the messages were not personal property, but were an inherent part of the office environment. Additionally, the court held that even if there were some expectation of privacy, a reasonable person would not find the invasion of privacy highly offensive, because the plaintiff had told the employer that the personal folders contained information relevant to the sexual harassment investigation.

4. Intentional Infliction of Emotional Distress (Legal Limits Management on Curiosity).

In most states, a person who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another is liable for resulting emotional distress or physical harm. RESTATEMENT (SECOND) OF TORTS, § 46. Many employees have asserted claims for intentional infliction of emotional distress based on an employer's review of e-mail messages they considered private. To date, the courts have universally rejected these claims. However, in appropriate circumstances, e-mail monitoring could lead to valid emotional distress claims. For example, a manager who assured employees that e-mail messages would be private, but then monitored those messages and divulged personal information to others in the workplace might be liable for intentional infliction of emotional distress if the employee learned of the disclosure and suffered emotional distress as a result.

5. Non-Solicitation Policies Under the National Labor Relations Act.

The use of e-mail raises difficult and unresolved issues under the National Labor Relations Act that are beyond the scope of this paper. While the Board has not directly addressed the issue, the General Counsel for the NLRB has taken the position that e-mail use on break time is nothing more than standard employee speech, and cannot be restricted at all.

C. Recent Legislative Efforts to Restrict Employer Monitoring.

In 1999, the California legislature passed a bill that would have prohibited employers from secretly monitoring e-mail or other personal computer records generated by employees on company systems. 1999 Cal. S.B. 1016. Before inspecting such records, the bill required that employers prepare and distribute a workplace privacy and electronic monitoring policy, and obtain a signed acknowledgment from every employee. Each policy was to provide a means for employees to review any information gathered from their computers or e-mail accounts, and the right to dispute the accuracy of collected data. Any employer who reviewed employee records without first obtaining a signed acknowledgment form, or who conducted a review in a manner that violated its own policy, was guilty of a misdemeanor.

On October 10, 1999, Governor Gray Davis vetoed the bill. His veto message stated that his decision was based on the common-sense presumption that employees in today's wired economy understand that computers provided for business purposes are company property and that their use may be monitored and controlled.⁶ He further reasoned that the bill was a trap for the well-meaning but unwary employer⁷ who was attempting to prevent improper e-mail use, including harassment and defamation.

D. Simple Steps to Avoid Liability (and Improve Efficiency Too!)

1. Defeating the Expectation of Privacy: Written E-Mail Use Policy.

- a. A model information technology policy.

[Company Name] provides desktop computers, pagers, computer software, e-mail and Internet access to employees to assist them in performing their job duties. These items are company property, and may be used only for business purposes. Inappropriate use of company property, including transmitting, receiving or downloading items that may be offensive to other employees is strictly prohibited, and may result in discipline, up to and including discharge.

The company has the ability to access and read any e-mail or pager message sent, received or transmitted using company equipment, and can also determine the Internet address of any web site accessed on company computers. The company will review and monitor employee use of these systems as it deems necessary to ensure that work time is used for work, and to maintain a professional and

appropriate work environment. Employees should not send or receive any private or personal information over these systems, because all messages and information may be reviewed by management. This is true whether or not you use a password to access an individual account.

All employees are expected to comply with all copyright, trademark and similar laws in connection with their use of the company's computer and telecommunication systems. Information available on the Internet may be subject to copyright protection, and shall not be used in a way that violates any existing copyright.

To maintain the confidentiality of company information, employees should not photocopy restricted or sensitive data, nor should they transfer such information to computer disk, or transmit it outside of the company via e-mail or facsimile without express permission for a business purpose. Confidential information includes [insert here.]

ACKNOWLEDGMENT

I have read and understand the company's Information Technology policy.

Signature

Date

- b. Additional areas you may wish to cover in your policy.

The above policy prohibits all personal use of company e-mail and Internet access. Where an employer desires to allow some personal use, the policy may provide: ~~A~~Occasional use for personal matters is permitted, but employees should be aware that all use may be monitored. Any inappropriate or excessive use will result in discipline.@

Policies may also address such issues as who may speak or write on the Internet as a representative of the company, and may also include a prohibition against any attempt to defeat or circumvent firewalls or

other security measures and distribution of chain letter, viruses, worms, trap-doors, etc.

- c. Caution! If you write it, you actually have to enforce it.

Policies are helpful in providing guidance to employees and in setting legitimate expectations. However, employers who commit to certain rules but fail to enforce them often find themselves in a more difficult position than they would have been in without any policy at all. An employer may do more harm than good to its chances in court if it commits to monitor e-mail, but fails to do so.

2. **Company-Wide Meeting.**

- a. What to say, and what to leave out.

In *Schwenn v. Anheuser-Busch*, *supra*, the plaintiff complained that she had received sexually explicit and harassing e-mail messages. The court ultimately dismissed plaintiff's complaint, noting that the plaintiff received the messages over a short period of time, and that upon receiving the complaint management immediately called a company-wide meeting to discuss proper use of the e-mail system. A proper response to any complaints will certainly make the courts more willing to view employers favorably when faced with employee allegations of harassment.

Key elements for a company wide meeting include the following:

- ✓ Review the anti-harassment policy.
- ✓ Explain that the policy covers inappropriate e-mail.
- ✓ State that the company will audit e-mail messages.
- ✓ State that inappropriate messages will result in discipline or discharge.
- ✓ Do not identify the complainant, if any.
- ✓ Do not promise more than you are actually going to deliver.

3. Investigating Complaints.

- a. How to do it and what to avoid.
 - ✓ Designate a limited number of responsible, trained individuals to receive all complaints of harassment.
 - ✓ Make a written note detailing all complaints received, no matter how minor. Preferably, ask the complainant to put the concern in writing.
 - ✓ Investigate promptly.
 - ✓ Get a printout of all e-mail messages or Internet sites visited on the computer of the alleged harasser. Know that if you don't do it, a plaintiff's attorney will.
 - ✓ For serious complaints, consider the use of a paid administrative suspension to remove the alleged harasser from the workplace.
 - ✓ Inform the complainant of the results of the investigation.
 - ✓ Do not promise complete confidentiality. Rather, state that you will only provide information to those with a need to know.
 - ✓ Do not agree to "just listen."

II. Internet Access.

A. Employer's Right to Monitor and Restrict Access.

In one recent case, *United States v. Simons*, 29 F. Supp. 2d 324 (E.D. Va. 1998), the CIA determined that one of its employees had been downloading child pornography from the Internet. The employee challenged the search of his hard drive as unconstitutional. The court first held that there was no constitutional violation because the employee had no reasonable expectation of privacy. The basic expectation of privacy an employee may have in a desk or office can be reduced by

actual office practices and procedures. Here, the CIA had an Internet use policy that specifically provided that the agency would monitor use and had the capacity to determine what web sites employees had visited. Additionally, the court stated that even if there had been an expectation of privacy, the search was reasonable in scope and execution, and so would not have amounted to a violation of the employees' rights.

Virginia has enacted legislation prohibiting state employees from downloading or storing sexually explicit information from the Internet. Professors at several state-run universities challenged the statute, arguing that it violated their First Amendment rights by inhibiting their ability to perform their employment duties, including assigning online research to students, accessing sexually explicit Victorian poetry, or researching issues of human sexuality. The district court initially granted summary judgment to the plaintiffs. In *Urofsky v. Gilmore*, 167 F.3d 191 (4th Cir. 1999), the Fourth Circuit reversed the decision, and granted judgment to the state, holding that the statute restricted the plaintiffs in their capacity as employees, and not as citizens addressing matters of public concern, and thus did not implicate First Amendment rights. The panel decision was vacated, and the case has now been reheard en banc, but a final decision has not yet been issued.

B. Recommended Policies.

See Model Information Technology Policy, above.

III. A Word About the Old Fashioned Stuff: Video and Audio Surveillance.

A. Stricter Limits.

1. Audio Surveillance of Oral Communications.

The Federal Wiretap Act prohibits the interception or disclosure of oral conversations by an individual not present at the time, if the participants had a reasonable expectation that their conversation was private. 18 U.S.C. §§ 2510-2511. Many courts have held that employees can reasonably expect that their conversations are private while at work.

In *Dorris v. Absher*, 959 F. Supp. 813 (M.D. Tenn. 1997), the Director of Rabies Control activated a Sanyo cassette recorder and placed it on the top shelf of a storage room. The recorder captured the conversations of several employees. The employees exhibited a subjective expectation of privacy by

not speaking when others, including members of the public were present. The court held that the employees reasonably expected that their conversations were private as to persons not present, and granted summary judgment on their federal wiretapping claims. *See also Desilets v. Wal-Mart Stores, Inc.*, 171 F.3d 711 (1st Cir. 1999) (manager's use of voice activated tape recorder to capture private conversations of night-shift employees violates federal Wiretapping statute).

2. Telephone Monitoring.

Under the federal Wiretap Act, employers normally will need to obtain employee consent for any ongoing monitoring policy. Employers can obtain implied consent by clearly and unambiguously notifying employees that calls on particular telephones will be monitored. The best approach is to obtain employee signatures acknowledging a written monitoring policy. Once a conversation is identified as a personal conversation, monitoring must cease. A more narrow exception to the federal rule, known as the business extension exception, permits employers to listen in on a regular extension line if the employer has a legitimate business purpose, and the employer does not listen to personal conversations. *See, e.g., Briggs v. American Air Filter Co.*, 630 F.2d 414 (5th Cir. 1980) (employer suspected employee was passing confidential information to a competitor, and knew employee was on the telephone with the competitor); *Berry v. Funk*, 146 F.3d 1003 (D.C. Cir. 1998) (business extension rule does not apply where policy states that calls will not be monitored without the employee's knowledge).

Various state laws include stricter requirements. Several states require that all parties to telephone conversations consent to monitoring or recording before it may take place. *See, e.g.,* FLA. STAT. ANN. ' 934.03(d).

3. Video Surveillance.

In locations where employees have a reasonable expectation of privacy, video surveillance will violate the common law of most states. Statutes in several states prohibit employers from installing cameras or other equipment for visually monitoring employee restrooms, locker rooms or changing rooms. *See, e.g.,* CAL. LABOR CODE ' 435; N.Y. GEN. BUS. LAW ' 395-b (the California law is directed at employers specifically, and the New York law covers businesses generally).

B. Permitted Uses.

1. Audio Surveillance of Oral Communications.

Under federal law, a person may record an oral conversation only if he or she is a party to the conversation. In short, you can wear a wire, but you cannot Abug@a room.

Best practice: if a conversation is to be tape recorded, the recording device should be placed in plain sight of everyone involved in the conversation, and the person making the recording should identify himself or herself at the beginning of the tape and obtain taped verbal consent for the recording from each person in the room. As a practical matter, tape recording is rarely if ever a good idea. Generally, it is better to simply have a reliable witness to important conversations.

2. Telephone Monitoring.

Employers in most states can safely institute telephone monitoring policies by providing written notice to employees and requiring their signatures on an acknowledgment and consent form. Monitoring should only be for legitimate business purposes, and whenever management determines that a call is personal in nature, monitoring on that particular call must cease.

Employers in states such as California and Florida, that require notice and consent from all participants to a telephone conversation prior to monitoring, will need to employ recorded message or have all employees read a script prior any conversation that may be monitored or recorded. Employers calling such states, or receiving calls from those states should also consider notifying customers that calls may be monitored or recorded, because in some cases the courts may apply the law of the customer-s state, rather than the business/employer-s state in determining whether monitoring or recording was legal.

3. Video.

In *Vega-Rodriguez v. Puerto Rico Telephone Co.*, 110 F.3d 174 (1st Cir. 1997), the employer initiated continuous video surveillance of its Executive Communications Center. The facility was a large, open space with no individually assigned desks or cubicles, and the cameras did not record sound

Communications Technology in the Workplace

or cover break areas. The plaintiffs challenged the recording as a violation of the Fourth Amendment, but the court found that the physical layout of the room defeated any reasonable expectation of privacy. The court also recognized the employer's legitimate desire to monitor employee productivity and to enhance security.