

Privacy and Profitability in the Technological Workplace

DENNIS R. NOLAN*

University of South Carolina, Columbia, SC 29208

I. Introduction

The labor law and human resources literature of the 1990s was replete with warnings that employers used modern technology to keep an eye on their employees. Computers monitored work performance, we were told; software programs tracked Internet usage; supervisors read employees' e-mail; and soon "smart badges" would reveal our exact location at every instant. These efforts even touched employees' lives away from work, as some employers searched the contents of computers they provided to telecommuting workers. Many of these articles and books adopted distinctly unscholarly tones of high dudgeon and alarm (Lee, 1994; Gantt, 1995).

The warnings were true, but they no longer surprise anyone. By now every sensible employee knows or should know that employers do or at least may use all the tools of modern technology to supervise and direct them. Indeed, smart employers go out of their way to tell employees about company policies on monitoring and on use of communications systems precisely in the hope that doing so will improve productivity and prevent problems. Nor is it any longer surprising that the law provides little protection for employees. Despite some initial uncertainty, despite volumes of academic criticism, federal and state courts soon reached a strong consensus that constitutions, statutes, and the common law provide few remedies for those subject to employer inquiry and observation. Legislatures have not, for the most part, changed those rules.

Where do those developments leave the commentator on workplace privacy? Simply repeating the old formulas would be pointless overkill. Even the recommendations for new judicial or legislative rules have a tired familiarity. Perhaps it is time to take a step back for the sake of perspective, to recount just what employers do, why they say they do it, and to compare their objectives with their methods. Because many of the asserted reasons relate to the law, it will also be necessary to outline how little the law requires or forbids and how much it permits. But the law, we shall see, is really a fairly minor player in this pursuit. Policies—business policies and personnel policies and even political policies—are far more important.

Those matters—employers' practices, the explanations for those practices, and the controlling legal requirements and prohibitions—comprise the heart of this explo-

ration. The following three sections cover each in turn. The final substantive section tries to distill lessons from the evidence. It addresses the oft-asked question, *What Then Must Be Done?*

II. *What Do Employers Do?*

Observation of employees is nothing new. Supervisors have always monitored their subordinates to make sure they worked steadily and well. All that has changed with the advent of the computer are the techniques and effectiveness of the observations. (I am primarily concerned herein with electronic monitoring; video and audio recording represent older and less controversial technologies, ones whose major issues were long ago resolved.) The new methods include monitoring work performance by means of software programs that record computer use, customer service contacts, and the like; limiting and monitoring employees' use of e-mail systems; limiting and monitoring employees' Internet use; and examining the stored contents of employees' computers. A recent survey by the American Management Association (AMA, 2002) provides a convenient look at the prevalence of these modern practices.¹

Averages aside, individual employers' policies on privacy and on use of electronic technology resources vary widely in detail and theme. Some provide lengthy rules that emphasize restrictions on employee activity (e.g., Archdiocese of Baltimore, 2002; Florida State University, 2002). Florida State's Information Technology policy, for instance, prints out to nine pages, most of which are devoted to detailed lists of requirements and prohibitions. The brief section on "Privacy and Security" first states that the University cannot guarantee that it will retain all critical data. The only other paragraph under that heading paradoxically provides that "unauthorized access" to computer files, "either by direct examination or by automated searching," will not be permitted "unless there is reasonable cause and access is approved by the director" of the facility supporting the system — unauthorized access, in other words, is prohibited unless it is authorized.

Other employers have briefer policies that give more weight to employees' privacy. A good example is the University of Southern California (2002), which bluntly states that it will not interfere with communications merely because they offend some viewers:

Section 3. Responsibilities and Privacy

3.1 . . . The university cannot and will not attempt to protect individuals from material that may be offensive to them, except in cases of violation of the law, university policy, or standards, and in these cases only where technically feasible. Individuals making use of electronic communications are warned that they may willingly or unwillingly receive or discover material they find offensive. The university will not establish additional standards, beyond those that are legally relevant, for discussion or language in electronic communication, including all forms a [sic] digital media. . . .

The University of Michigan's policy is similar: "Censorship is incompatible with the goals of an institution of higher education. Research and instruction take many

forms. Therefore, information accessible on the network may not be restricted through censorship" (University of Michigan, 1997).

Still other employers, for example my own University of South Carolina, say little one way or another. South Carolina's computer policies (University of South Carolina, 1995, 2002) deal primarily with access and security issues; while they warn that sending obscene messages is illegal under state law, the focus is on the proper procedure for reacting when one receives such a message. They say nothing about monitoring or content restrictions.

Computerized Monitoring of Work Performance. Use of computers to monitor employee performance is a natural extension of earlier methods for tracking employees' work. Consider a simple assembly line. As far back as Henry Ford's time and probably before, supervisors stayed near employees and watched their work. Piecework systems made precise recording more important, so workers themselves often completed the necessary records or made appropriate notes on tickets attached to work orders. New machines enabled employers to scan such records into computer data bases. From there it is just a short step to having employees enter the information into computers themselves, so that their effort and results could be tracked automatically. The differences between traditional monitoring by supervisors and modern monitoring by computers is thus one of style, not of kind. To be sure, computers don't nod as often as supervisors do, but it would be hard to argue that employees had a right to inefficient supervision.

Relatively few employees today work on traditional assembly lines. Many more work at computer terminals, handle telephone calls, make deliveries, or sell hamburgers or televisions in retail operations. Continuous monitoring in those cases is simple. Software programs can record and analyze the number of keystrokes, the percentage of time the computer is used, the number and duration of calls received, the time of each delivery, and the value of sales. Supervisors, who may not even be within sight, can track employees' performance by the minute. Software programs can even alert employees about their performance compared to stated expectations or to their co-workers' activities.

A decade ago, this seemed vaguely Orwellian. Some writers even warned about the developing "electronic sweatshop" in which employers would constantly raise demands based on their ability to determine what the most efficient employees could do (Boehmer, 1992; Lee, 1994). Today computer monitoring is standard practice in many industries, including telecommunications, insurance, and marketing and customer care departments of retailers and service providers. According to the AMA survey, 43 percent of employers record telephone statistics (time spent and numbers called) while nearly 19 percent record computer use (time logged on, keystroke counts and the like). No doubt many employees work harder or more consistently today than they did with less supervision, but their additional work has not yet produced the predicted "sweatshop."

One new development, however, is that these modern monitoring practices even touch professionals who have long been exempt from close scrutiny. Managed-care providers, for example, require detailed records of doctors' consultations with patients, tests ordered, prescriptions written, and so on. Lawyers routinely and carefully track time spent on the telephone or on Westlaw for each client, both for internal purposes and to provide accurate records for client billing. All such records are either entered directly into a computer or are promptly transcribed. All can be analyzed by computer for later review by employers or others. Comparable monitoring methods affect other professions as well. Not only is computerized monitoring more efficient than older styles of supervision, it is also more far-reaching.

Limiting and Monitoring E-Mail. E-mail is now a universal method of business communication, more common in many workplaces than telephones were just a few years ago. Like telephones, e-mail systems are subject to abuse by employees. Someone who formerly called a friend or family member to chat for a few minutes during the work day may now just exchange e-mails. And as with telephones, employers have tried to monitor and control e-mail use. E-mail monitoring ranges from innocuous to absurd, with some rational activity in between.

Sophisticated e-mail systems automatically store incoming and outgoing messages, so mere recording of transmissions is not a serious privacy issue. In fact, it can even be a convenient way for senders and receivers alike to retrieve needed communications. Privacy concerns arise only if someone else reviews one's stored e-mail messages. The AMA survey reports that nearly 47 percent of employers did so in 2001, more than double the 1998 percentage. Given the enormous volume of e-mail messages, however, employer review must either be sporadic, narrowly targeted, or restricted to a small sampling.

As with telephones, employers have found personal use of e-mail almost impossible to control. Most have resigned themselves to allowing some personal e-mail use, just as they permit some personal telephone calls. Florida State University, for example, recognizes that "Occasional, incidental personal use of IT resources is permitted" subject to certain limits. Some, though, still try to prohibit all nonbusiness use of the employer's e-mail system. The Archdiocese of Baltimore limits "personal use of the Internet Facilities and equipment to that which is incidental to the User's official assignments and job responsibilities."²

When e-mail was new, an absolute prohibition on personal use might have seemed feasible; now it certainly does not. Separating business and personal messages is no easy task. When communicating with co-workers, suppliers, and customers, employees often mix personal topics with professional ones; indeed, they may not perceive any bright line separating the categories. Routine employer review of e-mails might not disclose which is which, and anything more than routine review would require more managerial time and effort than the risks of lost work time would justify. Moreover, a blunt prohibitory approach or widespread monitoring could easily create morale problems and would certainly pose difficult enforcement decisions (Mignin et al., 2002).

More limited employer use of stored e-mails — for example, as part of an investigation into alleged fraud or harassment — makes more sense on both sides. For employers, it is far less costly than routine review, and far more likely to produce useful results. For employees, it means that few of their messages will ever be seen by a manager.

As an alternative or as a supplement to active monitoring of e-mail, some employers use filters that detect and delete messages containing “improper” words, or else alert and warn employees when such words are detected. When used simply as a caution to employees, such computer “flags” might make sense. An occasional alert might deter employees from using insulting or offensive language. Deterrence is one major reason why many employers put “splash screens” on office computers that restate some computer policies every time an employee boots up.

Some of these programs, however, are simply silly. One recent newspaper report described software used at a North Carolina high-tech company. This “cyber-censor” blocks e-mails containing offensive words. “Instead of the whole message, the sender receives a list of the swear words it contains, along with an explanation (e.g., ‘dirty word’ or ‘sexual discrimination’) of why they are offensive” (*Independent Weekly*, 2002, p. 3). Like most other computer filters, this one had some strange quirks that caused it to ignore some offensive language while flagging some perfectly harmless terms.³ Rosen (2000, pp. 57-58) reports that George Washington University’s law school, where he teaches, mistakenly installed an e-mail censorship system on computers in the library. “Students who typed the word ‘drugs’ on their university e-mail accounts . . . were automatically logged off the network with a stern warning.”

The inaccuracy of e-mail and Internet screening programs is legendary. Every reader subject to screening could probably supply comparable examples. One has to wonder whether the benefits are sufficient to outweigh the inconvenience caused by the errors, even leaving aside the harm to an employer’s image caused by clumsy screening.

Even when employers themselves do not read employees’ e-mail messages, others might. In several recent instances, journalists and litigants have used state open-records laws to gain access to messages that senders never thought would go beyond their intended recipient. After a University of North Carolina at Wilmington professor, using his university computer, criticized a student’s attacks on America’s foreign policy on the Middle East, the student accused him of defaming and intimidating her. She sought copies of the professor’s e-mail messages. University administrators reviewed his correspondence to determine if any were “public records.” They decided none was, so they released only a log rather than the complete messages. Even so, the professor’s correspondence was viewed by unanticipated people, and the prying student learned at least the addressees and times of the messages. A case in Tennessee was even more intrusive. A local newspaper obtained and published e-mail messages between the University of Tennessee’s former president and a subordinate with whom he apparently had an affair. Some of the messages were so intimate that one blushes to read them, not that questions of taste would limit a modern newspaper.

Both of these cases are described in Foster (2002). The title of her article, "Your E-Mail Message to a Colleague Could be Tomorrow's Headline," aptly sums up the current situation for local government employees. Private sector workers are not so exposed to the scrutiny of outsiders, but even their communications are reachable in the course of litigation or other investigations.

Limiting and Monitoring Internet Usage. Widespread employee access to the Internet is a newer phenomenon. As a result, employer monitoring was late in arriving. By 2001, however, over 62 percent of the AMA respondents monitored their employees' Internet use, up from 54 percent the previous year. The software programs available for Internet monitoring are simple and revealing. They can bar access to certain sites, alert employees that the accessed site is prohibited or questionable under the employer's policy, or create a record for later investigation by the employer's information technology staff. One program informs employees that their attempt to access a certain site has been reported to the company's computer help desk. An employee with a legitimate explanation for the attempted access could then contact the help desk for permission. Those without a legitimate reason could be warned or disciplined. Net Tracker, a program sold by Computer Age Co., provides daily reports identifying every employee who accessed improper sites. If an employer wishes to investigate further, it can produce a detailed list of every site the employee visited and the time spent at each. With very little effort, the employer can even print out the very pages viewed by the employee. As evidence in litigation or arbitration, the results can be devastating.

The primary target of this monitoring, intentionally or otherwise, seems to be the employee who accesses pornographic web sites. Virtually all of the reported court and arbitration cases involved such activities. Spending work time shopping, gambling, planning a personal trip, playing solitaire, and reading lawyer jokes online is just as costly to an employer as viewing pornography, but the published cases seldom show discipline for those activities. Only sex sites, it seems, draw serious discipline. Perhaps it is just easier for employers and monitoring software to identify sexually oriented web sites as being distinctly unrelated to work. Their names alone tell a story. More likely, as the next section suggests, employers' concerns extend beyond lost time to questions of morality, and morality is far more often concerned with sex than with shopping.

Internet filters are at least as problematic as e-mail filters: both are over-inclusive and under-inclusive. A filter imposed by the Loudon County, Virginia public library was so broad that it blocked access to harmless sites run by Zero Population Growth and the American Association of University Women (Rosen, 2000, p. 85). A Virginia law restricted state employees, even university professors, from accessing or storing sexually explicit material on state-owned computers. Although a federal district court struck down the ban as a violation of the First Amendment, an appellate court ultimately found the ban Constitutional (*Urofsky v. Gilmore*, 2000). Similar restrictions have been upheld elsewhere (e.g., *Loving v. Boren*, 1997). As even high school students have demonstrated to their librarians, technologically skilled users have little difficulty evading filters. Still, their very existence may deter some misuse.

Examining Employees' Computer Files. Reviewing employees' computer files is much less common than the other forms of surveillance. Just over a third of the AMA respondents reported doing so in 2001, although the practice had nearly doubled since 1998. This may be surprising, given that individual computers are almost as "sticky" as e-mail systems. Many people still believe that deleting a file means that no one will ever see it again. They can be unpleasantly surprised to learn that almost nothing short of reformatting one's hard drive will truly eliminate a file. Widely available computer tools can locate and restore most supposedly deleted files.

Why then is review of stored files so much less common than other forms of monitoring? For one thing, reviewing hard drives is much more labor intensive than using an automatic filter on Internet usage. Employees may have thousands of files on their computers. File names may not obviously indicate contents, and there are simple ways to hide files from superficial monitoring. Unless one has a specific objective in mind and knows how to find the desired information, the chance of finding evidence of improper computer use would seldom be great enough to justify the effort — the game simply wouldn't be worth the candle. Moreover, even though employees' stored files on the employer's computer are legally no more private than their e-mail or Internet records, employees and employers alike might well regard hard-drive searches as more intrusive.

III. *Why Do They Do It?*

Employers offer — or writers offer on their behalf — several reasons for these sorts of investigations and restrictions. In addition, there seem to be a few plausible but dubious or even illegal unadmitted explanations. The "public" reasons center on profitability concerns, worries about loss of confidential information or compromising computer security, and fear of liability for employees' misuse of computers and communications systems (Mignin et al., 2002, p. 15). The "private" reasons include curiosity, morality, and union avoidance.

Profitability. Employers' profitability concerns involve the costs of the equipment and systems used by employees for non-work purposes and the time they lose from their duties. Equipment costs are impossible to estimate but likely to be extremely small. Once an employer has purchased a computer and necessary peripherals for an employee, employee misuse will not easily contribute to the equipment's depreciation. Cars and trucks rapidly deteriorate with use; computers normally don't. Obsolescence is a far more common reason than overuse for having to replace electronic equipment.

System costs from employee misuse are surely greater than equipment costs. Even so, the marginal cost of each additional e-mail message or Internet visit is trivial, far less than the cost of one personal long-distance telephone call. Only if large numbers of employees frequently used a large amount of bandwidth would the system costs of e-mail or Internet misuse be substantial (Kesan, 2002, pp. 314-15).

The real cost of such misuse comes from wasted time (Kesan, 2002, p. 314). While there are no hard figures available, the loss of work time while employees send personal messages or conduct personal business online must far exceed the minutes spent in the pre-computer age around the proverbial water cooler. One recent report indicated that half of all online shopping takes place at work (Mignin et al., 2002, p. 23). Another survey found that nearly a quarter of the online communications at responding companies was not work related. The most commonly visited web sites were those dealing with news, sex, investments, entertainment, and sports (Kovach et al., 2000, p. 295, citing Garofalo, 1998). It is therefore especially interesting that the reported cases do not show discharge or serious discipline simply for wasting time on non-work messages or sites. It may be that lesser actions such as counselings, which are not typically litigated or arbitrated, keep the problem to tolerable levels. Combine wasting time with sex, however, and employers react more strongly.

Security. An oft-cited justification for monitoring and system restrictions is the fear that employees will intentionally or inadvertently disclose confidential information, download or spread computer viruses, or otherwise compromise computer security. The explanation is plausible, at least until one tries to match it up to the means used. Unless managers consistently, thoroughly, and simultaneously review their employees' e-mails and Internet usage, monitoring could not prevent security problems. Screening programs do not distinguish between confidential and nonconfidential information. Viruses can and usually do arrive on any download, even those that sound innocuous. Virus scans are more effective and less intrusive "inoculations" than are a supervisor's eyes. Carefully restricting access to an employer's own confidential files or computer programs will do far more good than trying to read e-mails or block specific web sites. To put it in other words, the chosen tool is not likely to complete the task.

Fear of Legal Liability for Employee Misconduct. Three types of employee misuse of electronic communications systems and computers threaten employers with potential liability. First, employees may use these systems for their personal financial gain. The problem is most common in financial services businesses like investment companies and banks. Second, employees might use the employer's facilities to violate intellectual property laws by copying or distributing protected material such as software programs, movies, and music. Third and perhaps most importantly, employee misconduct might contribute to sex or race discrimination, particularly by fostering a "hostile work environment." These risks would exist even without computers, but the technological workplace exacerbates the problems by making violations so easy. A stockbroker, for instance, could shift a client's funds with a few clicks; there is no need even to forge a check. Copying videos or songs is now simpler than photocopying a text book used to be. Offensive jokes and cartoons that used to be passed hand to hand can now show up in a company-wide message.

Again, however, the literature of actual cases shows few disciplines for financial or copyright abuse. There have been no cases comparable to the litigation brought a

few years ago by textbook publishers against a major photocopying concern that helped professors create course materials without the burden of getting copyright permissions. Even within the hostile work environment category, sexually oriented e-mails and downloadings prompt discipline and litigation far more often than, say, racist communications. It is not clear why this should be so. Perhaps sexual activity, a primal force, is more pervasive than racism, or perhaps women are more likely than racial minorities to perceive and challenge a hostile work environment. Perhaps employees complain to employers more readily about the former than about the latter. More likely, sexual materials, particularly graphic materials, are of wider interest and thus are distributed more widely; if so, they naturally would draw more managerial attention.

Curiosity and Morality. Employers are not likely to admit to less "business-like" explanations for monitoring or restricting employee e-mail and Internet use. After reviewing the cases and the literature, however, it is hard to escape the conclusion that some employers are simply curious, voyeuristic, or moralistic about their employees' conduct. The monitoring methods they use are so ill-suited to achieving other objectives that one has to be suspicious of their real motives.

The predominance of discipline for sex-related communications enhances that suspicion. More people use employer-provided e-mail and Internet service for other sorts of personal purposes, yet only those whose usage somehow involves sex seem to get fired. Fear of liability for creating a hostile working environment does not completely explain that disproportion. Most of the reported discharge cases involve either a single individual's Internet usage or communications between consenting adults, not complaints by unintended viewers. The chance that sensitive employees may inadvertently see such private communications may partially explain employers' concentration on these offenses but, at least in light of the minimal risks discussed in the next section, their responses look like overkill. Most of the reported arbitration cases mention violation of an Internet policy as the reason for discipline, not vicarious liability.

Suppose instead that some employers simply want to know what employees are up to. That would explain routine monitoring even when there are few practical risks of liability. In the same way, if some employers think that employees exchanging dirty jokes and looking at *Penthouse* Playmates is immoral, while keeping in touch with old friends or buying DVDs is not, both their methods and their reactions to discoveries make sense. They may logically punish the one but not the other.

But the search for a single explanation is unfairly reductionist. No doubt most employers act out of a host of motives, some real, some exaggerated, some questionable, and some quite unconscious. Curiosity and morality may simply be among the questionable or unconscious kinds. Even so, they could enhance employers' eagerness to adopt and enforce policies dictated by other, more legitimate considerations.

Union Avoidance. No smart employer will ever admit to using its communications policies to interfere with employees' rights to unionize. Nevertheless, as Malin and Perritt (2000) have shown, some do just that. Restrictive policies can be overt (as by pro-

hibiting messages about unions or working conditions) or more subtle (for example, by prohibiting all non-work messages with the specific intent of preventing union-related ones). Monitoring for union-related messages or web sites or for other communications that would fall under the National Labor Relations Act's protection of "concerted activities for . . . mutual aid or protection" (Section 7) would also violate the law.

The touchstones for NLRA Section 7 analysis are intent and unequal treatment. Any rules adopted specifically to inhibit collective activity would run afoul of that section; so would facially neutral rules that are enforced unequally. While less clear, it is at least arguable that e-mail communications on the employee's non-work time are entitled to the same protection as face-to-face communications, at least unless the employer can demonstrate a valid business reason for restricting e-mail communications more strictly than other forms of speech. If so, that would mean that under the NLRA, the employer could not lawfully prohibit communications during employees' free time. Because there is usually no measurable marginal cost to an individual message sent and received on the employees' own time, articulating a legitimate justification for a total ban would be difficult.

Thus an employer concerned solely about costs and efficiency might lawfully permit only business-related e-mail and Internet use during working hours. Permitting some nonbusiness uses during work time while prohibiting employee complaints about working conditions, in contrast, would certainly violate Section 7. Restricting e-mails during non-work hours with no demonstrable efficiency reason might also be illegal.

IV. *What Does the Law Require, Forbid, and Permit Employers to Do?*

Because employers primarily cite legal rules as the main justification for monitoring and restricting their employees' electronic communications, some discussion of the law is essential. It is not necessary or desirable here to parse all the statutes and cases. Others, notably Finkin (1995, 2002), have already done so well and at great length. Rather, a brief summary of the most significant points should suffice. In general, the law puts very few obligations on employers but allows them wide freedom. Accordingly, employers can largely choose how much or how little supervision of employee communications they will employ.

Legal Requirements. No law specifically obliges employers to evaluate employees' work by means of a computer, inspect their files, or monitor their e-mail or Internet activities. Many legal rules, however, place the employer at risk because of employee misconduct. Four clear examples include liability for employees' tortious activity, for their violations of copyright, trademark, and trade secret laws, for supervisory discrimination, and for employee-created work environments that are hostile to women, racial minorities, or other protected groups.⁴

(1) Under the doctrine of *respondeat superior*, employers can be liable for harms caused by an employee's wrongful act if the act occurred within the employee's "scope of employment" (an amorphous term to which courts have given broad mean-

ing) and if the employer knew or should have known of the wrongful act (Ishman, 2000, p. 125). If a brokerage employee manipulates stock prices by spreading false rumors and the employer has reason to know about the activity, the employer might be liable to those defrauded, as Merrill Lynch seems to be learning as this is written. If a bank employee misappropriates a client's funds and the bank should have known about the thefts, the bank itself might be liable.

(2) If employees infringe copyrights or trademarks, the employer could be vicariously liable even without actual knowledge if it had the right to supervise the employees and had a direct financial interest in the infringing activities. The liability would be even clearer if it knew of, induced, or contributed to the infringing conduct (Ibid., p. 135).

(3) Direct workplace discrimination does not require a computer. Supervisors can refuse to hire or deny a promotion often without a word; they can trade benefits for sexual favors without a keyboard. Nevertheless, e-mail correspondence can provide both plaintiffs and employers with evidence of misconduct. Monitoring e-mails might therefore be one way for employers to detect and cure problems before they rise to the level of a lawsuit.

(4) Employers' greatest vicarious liability worry today stems from the possibility that employees may create a "hostile work environment" that would amount to a form of sex or race discrimination. The relevant statutes, most importantly Title VII of the Civil Rights Act of 1964, were reactions to commonly understood forms of discrimination, such as refusal to hire or promote people because of their sex and race. They did not expressly address sexual harassment. In *Meritor Savings Bank, FSB v. Vinson* (1986), the Supreme Court first held that sexual harassment could also violate Title VII. Its rationale was that some harassment creates a work environment that limits women's employment opportunities just as severely as the older forms of discrimination. The Court suggested that employers could reduce their exposure by establishing procedures for preventing or redressing such harassment. Among the types of once-tolerated conduct that could contribute to a hostile work environment are unwanted physical contact, sexual propositions, innuendo, foul language, gender-related jokes, and the display of obscene material.

Not every offensive act or word constitutes actionable harassment. In the usual legal formulation, the conduct must be "sufficiently severe or pervasive to alter the conditions of the victim's employment and create an abusive working environment," *Meritor Savings Bank, FSB v. Vinson*, 477 U.S. 57, 67 (1986); see also *Harris v. Forklift Systems, Inc.*, 510 U.S. 17, 21 (1993). Isolated or minor incidents may become evidence of a discriminatory environment but usually will not by themselves prove its existence (Finkin, 2002, p. 147).⁵ The courts have not yet turned the anti-discrimination laws into a generalized code of workplace civility. Nevertheless, e-mail messages and other forms of communication, especially when combined with other evidence, can become sufficiently severe as to expose the employer to liability. For example, in *Blakey v. Continental Airlines* (N.J., 2000), the court held that an employer could be liable for a hostile work environment arising from allegedly defamatory statements on the employer's electronic bulletin board.

In two 1998 cases, *Burlington Industries v. Ellerth* and *Faragher v. City of Boca Raton*, the Supreme Court refined the law about an employer's potential responsibility for sexual harassment. It held that an employer is automatically liable for a supervisor's harassment that produces tangible job consequences, but that it might escape liability for harassment without such consequences if it promulgates and enforces a suitable sexual harassment policy and if the victim failed to use the policy to correct the errant behavior. Prudent employers reacted to these cases by prohibiting and punishing communications and conduct that might offend members of protected groups. That obviously includes overtly harassing communications but some employers now ban even relatively harmless speech and activity. Some (Rosen, 2000, pp. 81-82) would say that they have even overreacted to the point of "prohibiting far more speech than the law actually forbids."

These developments in sex discrimination law, along with extensions to the law of race discrimination, directly relate to the present topic. Employers understandably fear that offensive e-mails might later be evidence of a hostile work environment, or that unintended employees might inadvertently view offensive Internet sites accessed by less sensitive employees. To prevent some offenses and to establish their bona fides under *Ellerth* and *Faragher*, many employers have adopted or strengthened their prohibitions against sex-related messages and Internet use. The same developments and responses also help to explain why those forms of computer abuse draw more stringent punishments than other forms that simply waste work time.

In sum, risks of legal liability, particularly for harassment by supervisors or co-workers, give employers a strong incentive to prevent, discover, and correct employee misconduct, whether or not that misconduct involves computers. As plausible as this explanation for strict control of communications systems might seem at first glance, the solutions do not always match up to the actual risks. Leaving harassment issues aside for a moment, the other potential risks do not require general screening programs. Banks and brokerages might need to monitor their electronic communications with customers just as they randomly monitor telephone calls to insure quality of service. Implementing a screening program to detect arguably offensive words does not contribute measurably to that objective, and customer protection has little or nothing to do with the question of Internet access. Copyright infringement and comparable offenses are a little different because they could involve both Internet and e-mail use, and also stored computer files.

Once again, though, generalized screening programs seem more intrusive than necessary. Random monitoring or, in the case of video and music downloads, a narrow screening system for those uses would address the plausible risks while not otherwise encroaching on employees' privacy. A better explanation is needed to justify the side effects that accompany the communications restrictions adopted by so many employers.

To return to the knotty issue of sexual and racial harassment, the cure here also seems stronger than necessary to address the disease. Harassment does not occur when an individual acts alone, for example by downloading information no one else sees.

Nor does it occur when consenting adults exchange such information. In both situations, the offense, if any, is of the same magnitude as conducting one's shopping online or spending too much time in idle chatter — that is to say, it involves a possible misuse of time or facilities but not potentially serious financial liability.

The reason for greater employer concern over offensive messages or files is that they might be seen by nonconsenting others. An employee who passes by the desk of someone looking at a pornographic picture, another who borrows a computer and finds offensive documents, a third who accidentally receives a racist e-mail intended for someone else: These are the possible victims. To become victims with a real cause of action against the employer, the workplace conduct they find offensive must be more than sporadic; only "severe or pervasive" comments, pictures, or actions will create a truly hostile work environment. Though small, the risk to employers is real. Occasional misdeeds of these sorts could, cumulatively, create sufficient evidence to convince a judge or jury that the employer maintained a hostile work environment. For employers, then, the unmistakable message of the law is that they should prohibit and punish *all* communications and conduct that might offend other employees. One method they use is to monitor and limit electronic communications on employer-provided equipment and systems. As one recent article (Adams et al., 2000, p. 35) put it,

The fact is that because of these concerns and the increasing efforts of the plaintiffs' bar to sue employers based upon allegations of employee misconduct of one sort or another, the obligation of employers to "police" (probably not too strong of a word) the conduct of employees and life in the workplace has never been greater. The role of the employer has become more paternalistic than ever. In this context, it is not unreasonable to expect employers to use any and all available technologies to monitor employees' conduct.

To protect themselves from liability, then, employers need explicit and effective anti-harassment rules. It is not so clear they need general bans on particular words in messages or on access to particular Internet sites, let alone bans on all non-work electronic communications or continuous or frequent monitoring of employee communications. Employers could instead wait until they learn of a possible offense and then address the specific case to make sure it does not recur. Alternatively, and more safely, they could emphasize prohibitions against computer misuse, then engage in more limited screening or monitoring, and enforce the prohibitions with progressive discipline. Instead, employers are increasingly adopting far broader rules and enforcing those rules by firing offenders.

Why do employers do more than the minimum required to avoid legal liability, even when that "more" involves spying on all employees or restricting otherwise lawful activities? The answer lies in the relative exposure to liability. The chance of losing a hostile work environment suit, or even of having to defend against a meritless suit, is more than minimal. As the next section shows, the law does not protect employees' interests in the privacy of their electronic communications at work, so there is almost no risk of paying damages to the employees subject to strict employer monitoring and control. Absent a legal counterweight to sexual or racial harassment suits,

it is safer for employers to err on the side of intrusion and restriction than on the side of toleration: to do the former is almost costless; to do the latter could be expensive.⁶ By prohibiting certain words altogether, employers might prevent the rare case where those words would reach and offend a protected employee; by prohibiting employees from accessing web sites with sexual content, they might prevent the even rarer case in which inadvertent viewings would poison the work environment; by dismissing an employee who commits one breach, they remove a possible repeat offender and might deter others from such conduct.

Legal Prohibitions and Permissions. The basic legal *requirements* are relatively clear though a bit fuzzy at the edges. Determining what employers must *not* do is more difficult. Several distinctions complicate this portion of the analysis. First, governmental employers are subject to constitutional restraints while private employers (with the exception of those in the few states whose constitutions do not require "state action" to trigger constitutional rights) are not. Second, the degree to which states value employee privacy against employer interests varies widely across jurisdictions. Third, the sources of privacy protection (constitutions, statutes, and common law causes of action) also differ in some respects.

Notwithstanding those complications, one element pervades almost all privacy protections. This common touchstone dates back at least to *Katz v. United States*, a 1967 Supreme Court opinion. In a concurring opinion, Justice Harlan asserted that privacy rights exist under the Fourth Amendment only when (a) a person has a subjective expectation of privacy that (b) society is prepared to accept as reasonable. In the phrase that is now universally used, a plaintiff must demonstrate a "reasonable expectation of privacy." If a person does not expect a particular mode of communication to be private, or if society does not regard that person's subjective expectation of privacy as reasonable, there is no cause of action. That is largely true for statutory and common law suits as well as for constitutional claims. The concept has also influenced the shape of legislative protections: Legislatures tend not to protect employees or others in matters over which they do not expect privacy or in matters over which society does not believe they should have privacy.

The primary application of the reasonable expectation of privacy concept to workplace privacy occurred twenty years later in another Supreme Court decision, *O'Connor v. Ortega* (1987). In 1981, officials at Napa State Hospital searched the office of Dr. Magno Ortega, a psychiatrist at the hospital, as part of an investigation of alleged misconduct (some of the allegations involved sexual harassment). While conducting the search, they opened his locked desk drawers and went through his private file cabinets, seizing some clearly personal and irrelevant items as well as some public and relevant ones. Dr. Ortega sued under federal and state law. By a 5 to 4 vote, the Supreme Court allowed his case to proceed to trial, holding that the constitutionality of a work-related office search depended on a standard of reasonableness.

That much was a victory for the plaintiff, but the Court's opinion, written by Justice O'Connor but representing the views of only four justices, sharply limited the

ability of employees to prevail in such cases. While granting that Dr. Ortega had a reasonable expectation of privacy in his desk and file cabinets and that public employers had to act reasonably in both the inception and the scope of office searches, Justice O'Connor warned that particular office practices, procedures, or regulations may reduce otherwise legitimate privacy expectations. For example, some offices are so open to the public or co-workers that no expectation of privacy would be reasonable. Those determinations, she wrote, must be made on a case-by-case basis.

More importantly, Justice O'Connor wrote that whether a given search was reasonable, even when the employee legitimately expected the site to be private, required balancing the employee's expectation against the employer's need for supervision, control, and efficient operation of the workplace. If those employer interests are strong enough, she indicated, no warrant would be required either for investigatory or work-related but noninvestigatory searches of otherwise private spaces. Because the facts of this case were not clear enough to justify summary judgment, the Court remanded the case to trial.

In the end, nine long years after the Supreme Court's opinion, Dr. Ortega won a verdict of several hundred thousand dollars when a jury found that the hospital's search was unreasonable. On appeal (*Ortega v. O'Connor*, 1998), the Ninth Circuit Court of Appeals emphasized the importance of privacy even at work. Referring to the "state and unsubstantiated charges of sexual harassment" made against Dr. Ortega, the court wrote:

... we reject the proposition that government employers are allowed to search their employees' private offices ... and seize their *purely personal* belongings on the basis of the type of charges involved here. ... Nor, equally important, may such a search be conducted in the absence of specific reason to suspect that particular evidence of misconduct exists and will be found as a result of the search. ... A charge that a person has engaged in what may be offensive sexual conduct on one or more occasions does not make his or her entire personal and family existence fair game for indiscriminate and unrestrained governmental intrusion and examination. In any event, any search of private areas for evidence of such activities must at a minimum be based on a specific reason to suspect that particular evidence exists and that it will be found in the place to be searched; moreover, such a search must be carefully limited in scope, not only because of an historic respect for fundamental privacy but because of the need to insure that the search will not be "excessively intrusive."⁷

By then, however, the Supreme Court's plurality opinion had been widely accepted as establishing two key points. First, public-sector employees have no claims against their employers for office searches if they had no reasonable expectation of privacy. As the Supreme Court emphasized, particular office practices, procedures, or regulations may undercut an employee's expectation of privacy. Perversely, perhaps, that holding gave employers a strong incentive to prevent or destroy expectations of privacy — by establishing rules denying privacy, by requiring employees to consent to searches, and by frequently exercising their search rights. *United States v. Simons* (4th Cir., 2000), for example, held that a federal agency's Internet policy reserved the right to inspect

and monitor employees' use of the Internet. Even though the policy did not refer specifically to inspection of office computers, the Court of Appeals held that it was sufficient to deny the employee any reasonable expectation of privacy in his downloaded files. "This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private. Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use."⁸ *A fortiori*, if the employee has no reason to believe that his or her e-mail messages or Internet records are private, the employer has no liability for examining them.

O'Connor's second point was that even if employees had a reasonable expectation of privacy, the employer's business interests could outweigh their privacy interests. These interests could include insuring employee performance, preventing violations of the law, or investigating suspected wrongdoing. Whether a given business interest supersedes a given privacy interest naturally has to be decided on a case-by-case basis.

Later decisions extended those points from alleged constitutional violations by government employers to alleged statutory or common law violations by private employers, and from searches of desks to screening of e-mail and examinations of computer files. A few examples illustrate the progression.

Several courts have addressed the first part of the *O'Connor* approach, the question of whether an employee has a reasonable expectation of privacy when using an employer-provided communications system. Almost uniformly they have ruled against the plaintiffs on that point. In *Bohach v. City of Reno* (D. Nev., 1996), for example, a police department examined the contents of messages the plaintiffs had sent to one another over the department's computerized paging system. Based on the contents of those messages, the department initiated an internal affairs investigation.

The plaintiffs sued to stop the investigation, alleging violation of their constitutional rights and of federal wiretapping laws. The court assumed that they had a subjective expectation of privacy, if only because they would not otherwise have sent the damaging messages, but concluded that their belief was not reasonable. When the system was installed, users were informed that messages would be logged and that certain types of messages were prohibited. Moreover, anyone with access to a department computer could scan all the messages. As a result, said the court, the plaintiffs could not reasonably have expected full privacy in their communications. In reaching its conclusion, the court quoted one law review commentator who generally favored employee privacy rights (Lee, 1994, p. 148, n.2) to the effect that employees' interests in e-mail privacy would probably "fail the 'expectation of privacy' test since most users probably realize that a system administrator could have access" to their e-mail.

Suits against private sector employers for invasion of employees' claimed e-mail privacy have met the same fate. Decades ago, employers who wanted to retain the right to inspect employees' lockers learned that they could defeat any expectation of pri-

vacuity simply by telling employees that lockers were provided by the employer for their business-related uses and were subject to inspection. The contemporary equivalent is an electronic communications policy telling employees that information transmitted or stored on the employers' systems belongs to the employer and may be reviewed.

In *Garrity v. John Hancock Mutual Life Insurance Co.* (D. Mass., 2002), the employer's computer policy sent a similar message, bluntly stating that the company "reserves the right to access all E-Mail files." The two plaintiffs sent and received sexually explicit messages. When one of those messages reached a third employee who was not amused, Hancock investigated, discovered the offensive messages, and fired the plaintiffs. They sued for invasion of privacy, among other things, alleging that the company led them to believe that they could keep their messages private by using passwords and personal e-mail folders. The federal district court rejected their claim: simply by sending the messages to another person, the court held, the plaintiffs lost any expectation that the messages would remain private.⁹

To the same effect are earlier cases relied on by the *Garrity* court. *Smyth v. Pillsbury Co.* (E.D. Pa., 1996) ("[P]laintiff voluntarily communicated the alleged unprofessional comments over the company e-mail system. We find no privacy interests in such communications.") and *McLaren v. Microsoft Corp.* (Tex. App.-Dallas, 1999) (because messages stored in personal folders were first transmitted over a network accessible by third persons, even the use of a password did not manifest a reasonable expectation of privacy). The *Smyth* case is particularly instructive. Smyth asserted that Pillsbury "repeatedly assured its employees . . . that all e-mail communications would remain confidential and privileged" and that "e-mail communications could not be intercepted and used by defendant against its employees as grounds for termination or reprimand." According to the court, Smyth lost his expectation of privacy when he voluntarily sent his comments to his supervisor: "unlike urinalysis and personal property searches, we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management." To put it more simply, even if an employer tells its employees that their e-mails are private, believing that statement may not be reasonable. Even if the employee's expectation were reasonable, said the court, a reasonable person would not "consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy."

Courts have likewise ruled against plaintiffs on the second portion of the *O'Connor* approach, finding that an employer's business interests could trump even a reasonable expectation of privacy. As *Garrity* noted, federal and state laws oblige employers to maintain a harassment-free workplace. "Therefore, once defendant received a complaint about the plaintiffs' sexually explicit e-mails, it was required by law to commence an investigation." Similarly, *McLaren* concluded that even if the employees had an expectation of privacy, "a reasonable person would not consider Microsoft's interception of these communications to be a highly offensive invasion. . . . [T]he company's interest in preventing inappropriate and unprofessional comments, or even

illegal activity, over its e-mail system would outweigh McLaren's claimed privacy interest in those communications."

Thus the law in this field is relatively clear: In normal circumstances, employees do not have a reasonable expectation that their communications using an employer-provided system are private, but even if they did, the employer's interests in preventing, detecting, and punishing misconduct would supersede their privacy claims. The absence of any constitutional or common law prohibition on employer access to such communications suggests a corollary principle, that employers may monitor and restrict their employees' e-mails, Internet use, and computer files.

Statutory Issues. Nor do communications privacy statutes provide employees with much protection. At first glance, one might assume that statutory bans on wiretapping and the like would keep employers from reading private e-mails. On closer analysis, the laws contain gaping exceptions for just these circumstances.

The primary federal law in this area is the Electronic Communications Privacy Act of 1986, or ECPA, an amendment to the earlier federal Wiretap Law (which itself is Title III of the grandly-named Omnibus Crime Control and Safe Streets Act of 1968). ECPA's Title I broadly prohibits interception of electronic (and other) communications; Title II prohibits accessing stored electronic communications. Each of these contains exceptions that free employers to engage in virtually all the workplace monitoring they could want (Kesan, 2002, pp. 296-98; Adams et al., 2000, pp. 38-40).

Three exceptions in the earliest and broadest law, the federal Wiretap Law, are carried forward into ECPA's Title I, the "consent exception," the "provider exception," and the "business use exception."

- First, an employer is freed of liability if the employee consents to the interception. While an employee might impliedly consent to monitoring, knowledge of possible monitoring without more will not suffice. Thus a prudent employer who wants to eliminate any risk of a violation should implement a comprehensive and clear policy and require employees to agree to it.
- Second, the Wiretap Law exempts interceptions by a service provider that are made within the normal course of employment and for the purpose of rendering its services or to protect its rights or property. (An employer who provides e-mail and Internet access is apparently a provider for this purpose.¹⁰) Those purposes would include monitoring to ensure quality service and to prevent theft; they would probably also include monitoring to prevent other violations of the law such as harassment.
- Third, the Wiretap Law's business-use exemption excludes from the definition of a covered "device" certain standard equipment. Courts interpreting the business use exception have applied both a "content approach" that focuses on whether the intercepted

communications are personal or business-related (only the latter may be monitored) and a "context approach" that focuses instead on whether the employer had a sufficiently weighty and legitimate business purpose for its monitoring.

In addition to these Title I exceptions, Title II has its own "provider" and "user" exceptions. Employers with their own communications systems are "providers" for purposes of Title II (*Bohach v. City of Reno*). The "user" exception is roughly analogous to the other Title's "consent" exception.

Putting these exceptions together, it is evident that ECPA does not generally bar employers from contemporaneously intercepting their employees' electronic communications or from accessing stored communications. The law protects employees only from third parties, not from those who provide the communications services in question. The most recent legislative action in this field, the Communications Decency Act of 1996 (a portion of the broader Telecommunications Act of 1996), added a new provision expressly protecting from liability "any 'provider or user of an interactive computer service' who restricts 'access to or (the) availability of' indecent material or helps others gain the technical means to do so" (Krattenmaker, 1996, pp. 147-48). Thus federal law not only permits employer monitoring of electronic communications, it positively encourages some such monitoring.

Many states have adopted their own electronic communications privacy laws but because most of these track ECPA's language, they allow employers the same freedom granted by federal law. A few states have stricter provisions or require employers to notify employees about potential monitoring, but these laws have significant limitations. Some address only tape recording or telephone interception and thus do not apply to electronic communications. Others contain exceptions that negate any promise of additional protection for employee privacy. Connecticut's law, for instance, generally requires notification to employees but exempts monitoring "when the employer has reasonable grounds to believe that an employee is creating a hostile work environment or is violating the law or the employer's legal rights" (Kesan, 2002, p. 301).¹¹

Conclusion. Every branch of the law — constitutional, common, and statutory; federal and state — allows employers wide discretion to monitor, restrict, and inspect their employees' electronic communications and files. At the same time, several branches of the law, particularly federal financial regulations, intellectual property doctrines, and anti-discrimination laws, impose at least some risk of liability on employers for their employees' misuse of the employers' communications systems. Given the state of the law, it would be a strange employer indeed that opted to protect employee privacy rather than to invade it. The primary motivation behind employers' monitoring and restricting their employees' use of electronic communications is profitability. When profitability conflicts with privacy, the former will prevail to the extent permitted by law. As one recent study phrased it, "The profits inherent in increased worker productivity and less employer liability provide strong incentives for the employer to disregard employee privacy interests" (Kovach et al., 2000).

V. *What Then Must Be Done?*

Policy recommendations have taken two wildly irreconcilable positions. Almost without exception, those concerned with management interests have urged employers to adopt extremely restrictive and intrusive electronic communications policies. E-mail and Internet facilities, they urge, should be restricted to work-related purposes; employers should routinely screen employee communications, bar messages containing improper words, and prohibit access to inappropriate web sites. Employees who violate those restrictions should be fired or at least severely disciplined.

Many of the cases mentioned above reflect equally strict policies. A good example of what cautious management attorneys are recommending to their business clients appears in an article by two labor lawyers from one of the country's largest law firms, Jones Day (Towns and Girard, 1998, pp. 24-27). The authors make twelve recommendations to employers:

1. Integrate e-mail and other policies.
2. Limit use of technology to business purposes only.
3. Reserve right to review and monitor.
4. Notify employees that passwords do not ensure privacy.
5. Include notice and consent language.
6. Do not engage in privileged communications via e-mail.
7. Strictly define appropriate Internet use.
8. Prescribe penalties for failure to follow Internet policies.
9. Enforce policies in a nondiscriminatory fashion.
10. Consider whether blanket rules are too broad.
11. Protect employees from inadvertent violations of copyright laws.
12. Develop a comprehensive records retention policy.

Note that almost all of these recommendations involve restrictions and their enforcement. The only one that recognizes a possible limit on employers is number 10. The authors' explication of that recommendation makes it clear that their concern is with rules that might run afoul of the National Labor Relations Act, not with employees' privacy. The authors' explication of recommendation 7 illustrates the point: "... an employer's policy may provide that employees may access the Internet only through the employer's approved Internet access procedures. In addition, an employer may wish to restrict or prohibit subscribing to public mail forums, ListServes, discussion groups, and the like."¹² Most advisors also recommend that employers adopt filtering and blocking software and that they investigate all flagged messages and accesses.

Restrictive policies like these might seem to solve management's problems with Internet and e-mail abuse, but restrictive rules carry substantial costs. Tight limitations could easily inhibit beneficial communications. Even the best filters are clumsy and often inaccurate. Heavy-handed rules indicate a lack of trust and might well hurt

morale and team spirit. Enforcement would require managerial time and resources, and would necessitate difficult decisions. Does the employer really want to discipline its best sales person because of a few offensive e-mails that got into the wrong hands? Will it dismiss the CEO for accessing "unapproved" web sites? Should the employee who completes all assigned tasks quickly and well be punished for using spare minutes corresponding with friends? And if the employer does not apply its rules equally to all, how can it avoid allegations of discrimination brought by those it chooses to discipline? Furthermore, the discovery process in any subsequent suit could turn up information about others that the employer really would not want revealed.

Those questions assume that employers realistically can control their employees' electronic communications. In fact, the job may be impossible. E-mail in particular is so widespread among workers with access to a computer that trying to limit its use to business purposes is like trying to stuff the proverbial cat back into the bag. Employers are likely to be no more successful than they have been with counterpart rules governing telephone use.

Those in the opposite camp argue that employers should have extremely limited rights to monitor employee communications. Having lost their arguments in the courts, privacy advocates have lobbied for federal and state legislation. Their major effort occurred in 1993 with the proposed Privacy for Consumers and Worker Act (PCWA). While phrased as an effort to limit improper monitoring and reduce some of the ECPA exceptions used by employers, the effect of the bill would have been to make most routine monitoring impractical – in other words, to reverse the impact of the statutory exceptions and court decisions described above. In the face of immediate and heated opposition from employers (and even from the Clinton Administration's Department of Labor), the PCWA died in committee. A more modest bill, the Notice of Electronic Monitoring Act (NEMA), was introduced in 2000. Unlike the restrictive PCWA, NEMA would allow any monitoring provided the employer notified affected employees ahead of time. Even the notice requirements are complicated, however, and violations would be punished by heavy fines.¹³ NEMA has made no more progress than the PCWA.

In addition to court and legislative efforts, some commentators have appealed directly to employers to change their emphasis. At the end of his chapter on privacy at work, Jeffrey Rosen (2000, pp. 89-90) makes this earnest if somewhat utopian plea:

There is no reason for us to accept the passive view that all e-mail messages sent over a university or corporate network must be considered public rather than private. We should try instead to carve out backstage areas where people can joke, let down their hair, and form intimate relationships free from official scrutiny. Some studies suggest that 40 percent of e-mail correspondence is unrelated to work; rather than trying in vain to exert managerial control over a medium that lends itself naturally to informal, and even irresponsible, communication, companies and universities might instead set aside e-mail accounts and areas of their networks as private places where speech and communications cannot be invaded unless there is cause to suspect individual users of serious misconduct.

As Rosen goes on to recognize, "this effort to distinguish between public and private speech in the workplace is something that current law refuses to allow." There's the rub: Given the potential liability on employers who do not restrict some types of communications, asking them to create specifically "private places" in which employees can "let down their hair, and form intimate relationships" is simply unrealistic.

As is so often the case, there is a lot of room for alternative positions between these extremes. Employers are not going to give up their rights to monitor employee performance, to insist on productivity during working hours, and to prevent and correct abuses of communications technology. They might, though, tailor their policies to accomplish their objectives with as little harm to other interests as possible. Moreover, employees themselves can do a lot to prevent intrusion on their privacy.

The starting place is the recognition that the law does not, and probably will not and should not, treat employees' communications at work or on an employer's communications systems as if they were private speech in their own homes. With that understanding, employees should limit the amount of personal business they do at work, use cell phones and pay phones and personal computers when feasible rather than using the employer's systems, and advise others not to send potentially offensive messages (and avoid distributing any that do arrive). Technologically adept employees should consider encrypting any personal messages whose disclosure could prove embarrassing, using anonymous remailers, and using "cloak" sites when browsing the web (Nichols, 2001, pp. 1602-03; Rodriguez, 1998, pp. 1470-72). Abstinence may not be the only guarantee of electronic privacy at work, but it surely is effective.

Employers, on the other hand, can balance profitability and privacy by adopting only as much restraint and monitoring as is essential for accomplishing managerial objectives. By balancing employee and employer interests and thereby minimizing overt intrusions, employers should enhance morale while keeping costs low. As one thoughtful commentator put it (Kesan, 2002, p. 331), monitoring "should be narrowly tailored to satisfy business-related, administrative, or legal needs, and any review of personal e-mail ought to be limited to ensure protection of personal information." Education should be a major component of any sensible computer policy. Once employees know the employer's expectations, the reasons for them, and the methods the employer will use to accomplish them, there should be few abuses. Just learning that messages cannot really be deleted and that supervisors can easily review Internet usage would go a long way toward deterring misconduct. Where some controls are necessary, blocking filters are more effective and less disturbing than human monitoring. It is hardly necessary to add that any policy should be clear, precise, written, well publicized, and consistently but reasonably enforced (Adams et al., 2000, pp. 44-45).

VI. Conclusion

New communications technology inevitably creates new problems of privacy; think of the introduction of telephones (when party lines were common), faxes (which can lie in a room accessible by many people before reaching the addressee), and cell phones

(which allow bystanders to hear one side of seemingly confidential communications). Computer monitoring of performance, e-mails, and Internet access are no different in this regard. Each development requires adjustments.

Old wine in new bottles, perhaps. What seems to drive the differing responses to the new bottles is that the newest forms of communication present an illusion of privacy. Everyone soon understood the limits to privacy presented by telephones, faxes, and cell phones. When new, however, e-mail and Internet access seemed more protected. We can see bystanders who might hear our telephone conversations and read our faxes, but those who monitor the new technology might never be seen. They might not even be human. It would be easy indeed, in those early days of the new technology, to conclude that there were no monitors. One beneficial by-product of the attention given to recent cases, and of employers' recent efforts to publicize their electronic communications policies, is that fewer employees should harbor any illusions.

Many of the adjustments to the new technology reduce the scope of individual privacy. To some degree that is inevitable. If so, employers and employees alike can and should act to minimize the intrusions, employees by avoiding questionable use of employer-provided equipment and systems, and employers by adopting reasonable rather than draconian computer and communications policies. The temptation is great for employers to overreach; avoiding that temptation may well be a bigger challenge than the possibility of employee misconduct.

NOTES

¹I thank Holly Newell of the University of South Carolina Law School Class of 2004 for her diligent research on and editorial assistance with this article.

²The AMA's membership consists of the nation's largest employers, employing a quarter of the nation's work force. Moreover, larger companies are the most likely to use new technology and new managerial techniques. The survey's results therefore likely show the direction in which other employers are moving. Because most employers do not publish their policies for outsiders, learning the details of their rules can be difficult. The examples cited in this article come from quotations in court cases and from publicly available policies, chiefly from universities.

³Note the apparent inconsistency: personal use is limited to that which is "incidental to" — that is, somehow associated with — official duties. Personal use is allowed, in other words, only when it is not truly personal. This sort of self-contradiction is all too common among the computer policies I have reviewed.

⁴The screening system described in that article sounds much like a program called Assentor. According to Jeffrey Rosen (2000, p. 57), Assentor "screens every incoming and outgoing e-mail for evidence of racism or sexism or body parts. After assigning each e-mail an offensiveness score, the program forwards messages with high scores to a supervisor for review."

⁵Isman (2000) provides a thorough analysis of the law of vicarious liability in the technological age. See also Settle-Vinson (1998).

⁶See, e.g., *Harley v. McCouch*, 928 F.Supp. 533 (E.D. Pa., 1996) (one offensive reference in an e-mail did not constitute a racially hostile environment); *Owens v. Morgan Stanley & Co.*, 1997 WL 403454 (S.D.N.Y., 1997) (same); *Schwinn v. Anheuser-Busch, Inc.*, 1998 WL 166845 (N.D.N.Y., 1998) (noting that other hostile work environment cases involved conduct extending over several years, the court held that sexually harassing e-mail over three weeks did not amount to a hostile work environment under New York law).

⁶The state of discrimination law creates a difficult issue that is beyond the scope of this essay. The government could not constitutionally ban most forms of speech and communication simply because women or minorities would find them offensive. Nevertheless, Congress and state legislatures have made employers liable for tolerating such constitutionally-protected activity. As a result, employers are forced to restrict their employees in ways the Government could not do directly; the anti-discrimination laws thus provide an indirect route around the First Amendment. See Rosen (2000), particularly chapters 2 and 3.

⁷*Ortega v. O'Connor*, 146 F.3d 1149, 1163-64 (9th Cir. 1998), quoting the Supreme Court's *O'Connor* decision, 480 U.S. at 726.

⁸To the same effect is *United States v. Reilly*, 2002 WL 1163572 (S.D.N.Y., 2002). U.S. Department of Labor policies warned employees that "By using Government office equipment, executive branch employees imply their consent to disclosing the contents of any files or information maintained or passed through Government office equipment." Every time the defendant turned on his computer, he received this message: "Users have no right to privacy while using any government owned or leased information technology system, which includes workstations, . . . software such as word processors, Internet browsers, electronic mail etc." Against that background, the court held, Reilly could not demonstrate that he had a reasonable expectation of privacy in diskettes beside his office computer.

⁹See also *Mutick v. Glenayre Electronics* (7th Cir., 2002) (where the employer announced that it could inspect the laptops it supplied to employees. Mutick had no right of privacy in his computer). Even without an express policy restricting computer use, employees should know some things they shouldn't do. *Autoliv ASP, Inc. v. Department of Workforce Services*, (Utah Court of Appeals, 2001) (sending explicit e-mails on a company computer network "violated a universal standard of behavior").

¹⁰See *Bahach v. City of Reno*, 932 F.Supp. 1232 (D. Nev., 1996) (police department was a "provider" of electronic communications services).

¹¹For more detailed discussion of state regulations, see Settle-Vinson (1998, pp. 67-70) and Adams et al. (2000, pp. 40-41).

¹²For examples of comparable policy recommendations to employers, see Hubbard (1998, pp. 147-48); Ishman (2000, pp. 157-60); Kesan (2002, pp. 330-32); and Mignin et al. (2002, pp. 17-21).

¹³Many of the articles in the References discuss these developments. See particularly Kesan (2002, pp. 299-300), Frayer (2002, pp. 868-71) and Rodriguez (1998, pp. 1464-65).

REFERENCES

- Adams, Hall III, Suzanne M. Schetingr, and Stacey A. Feeley, "E-mail Monitoring in the Workplace: The Good, the Bad and the Ugly," *Defense Counsel Journal* 67 (January 2000): 32-46.
- Allen, Anita L. "The Wanted Gaze: Accountability for Interpersonal Conduct at Work," *Georgetown Law Journal* 89 (June 2001): 2013-28.
- American Management Association, 2001 AMA Survey, Workplace Monitoring & Surveillance, <http://www.amanet.org/research/pdfs/ems_short2001.pdf>, last visited June 3, 2002.
- Archdiocese of Baltimore, Computer Use & Internet Policy, <<http://www.archbalt.org/technology/info/policy.pdf>>, last visited July 2, 2002.
- Autoliv ASP, Inc. v. Department of Workforce Services*, 29 P.3d 7 (Utah App. 2001).
- Baum, Kevin J. "Comment: E-mail in the Workplace and the Right of Privacy," *Villanova Law Review* 42 (3, 1997): 1011-42.
- Beeson, Jared D. "Cyberprivacy on the Corporate Intranet: Does the Law Allow Private Sector Employers to Read Their Employees' E-mail?" *University of Hawaii Law Review* 20 (Summer/Fall 1998): 165-219.

- Blakey v. Continental Airlines*, 164 N.J. 38, 751 A.2d 538 (N.J., 2000).
- Boehmer, Robert G. "Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop." *DePaul Law Review* 41 (Spring 1992): 739-819.
- Bohach v. City of Reno*, 932 F.Supp. 1232 (D. Nev., 1996).
- Burlington Industries v. Ellerth*, 524 U.S. 742 (1998).
- Faragher v. City of Boca Raton*, 524 U.S. 775 (1998).
- Finkin, Matthew. *Privacy in Employment Law*. Washington, D.C.: Bureau of National Affairs, 1995 and 2002 Cumulative Supplement.
- Florida State University. OP-H-6, Use of University Information Technology Resources. <<http://www.vpl.fsu.edu/policies/manual/itpolicy.html>>, last visited July 2, 2002.
- Foster, Andrea L. "Your E-Mail Message to a Colleague Could Be Tomorrow's Headline." *Chronicle of Higher Education*, June 21, 2002.
- Frayer, Charles E. "Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests." *Business Lawyer* 57 (February 2002): 857-74.
- Gantt, Larry O. Natt H. "An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace." *Harvard Journal of Law and Technology* 8 (Spring 1995): 345-425.
- Garofalo, Beverly. "Sharing a Middle Ground with Big Brother." *Connecticut Law Tribune*, May 18, 1998: pp. 1-6.
- Garrity v. John Hancock Mutual Life Ins. Co.*, 18 IER Cases 981, 2002 WL 974676 (D.Mass., 2002).
- Harley v. McCouch*, 928 F.Supp. 533 (E.D. Pa., 1996).
- Hubbart, William S. *The New Battle Over Workplace Privacy*. New York: AMACOM, 1998.
- Independent Weekly*. "Cyber-cussing." May 15-21, 2002.
- Ishman, Mark. "Computer Crimes and the *Respondent Superior* Doctrine: Employers Beware." *Boston University Journal of Science and Technology Law* 6 (June 1, 2000): 115-62.
- Kat. v. United States*, 389 U.S. 347 (1967).
- Kesan, Jay P. "Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace." *Florida Law Review* 54 (April 2002): 289-332.
- Kovach, Kenneth A., Jennifer Jordan, Karen Tansey, and Eve Framinan. "The Balance between Employee Privacy and Employer Interests." *Business and Society Review* 105 (Summer 2000): 289-98.
- Krattenmaker, Thomas G. "The Telecommunications Act of 1996." *Connecticut Law Review* 29 (Fall 1996): 123-74.
- Lee, Laurie Thomas. "Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the 'Electronic Sweatshop'." *John Marshall Law Review* 28 (Fall 1994): 139-77.
- Loving v. Boren*, 956 F.Supp. 953 (W.D. Okla., 1997), affirmed on other grounds, 133 F.3d 771 (10th Cir., 1998).
- Malin, Martin H. and Henry H. Perritt, Jr. "The National Labor Relations Act in Cyberspace: Union Organizing in Electronic Workplaces." *University of Kansas Law Review* 49 (November 2000): 1-64.
- McLaren v. Microsoft Corp.*, 1999 WL 339015 (Tex.App., Dallas, 1999).
- Meritor Savings Bank, FSB v. Vinson*, 477 U.S. 57 (1986).
- Mignin, Robert J., Bart A. Lazar, and Josh M. Friedman. "Privacy Issues in the Workplace: A Post-September 11 Perspective." *Employee Relations Law Journal* 28 (Summer 2002): 7-23.

- Minick v. Glenayre Electronics*, 280 F.3d 741 (7th Cir., 2002).
- Nichols, Donald H. "Window Peeping in the Workplace: A Look into Employee Privacy in a Technological Era." *William Mitchell Law Review* 27 (3, 2001): 1587-1608.
- O'Connor v. Ortega*, 480 U.S. 709 (1987).
- Ortega v. O'Connor*, 146 F.3d 1149 (9th Cir., 1998).
- Owens v. Morgan Stanley & Co.*, 1997 WL 403454 (S.D.N.Y., 1997).
- Rodriguez, Alexander L. "Comment: All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace." *Emory Law Journal* 47 (Fall 1998): 1439-73.
- Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House, 2000.
- Schwenn v. Anheuser-Busch, Inc.*, 1998 WL 166845 (N.D.N.Y., 1998).
- Settle Vinson, Mia G. "Employer Liability for Messages Sent by Employees Via E-mail and Voice Mail Systems." *Thurgood Marshall Law Review* 25 (Fall 1998): 55-74.
- Smyth v. Pillsbury Co.*, 914 F.Supp. 97 (E.D. Pa., 1996).
- Towns, Douglas M. and Jeana Girard. "Superhighway or Superheadache? E-Mail and the Internet in the Workplace." *Employee Relations Law Journal* 24 (Winter 1998): 5-29.
- United States v. Angevine*, 281 F.3d 1130 (10th Cir., 2002).
- United States v. Reilly*, 2002 WL 1163572 (S.D.N.Y., 2002).
- United States v. Simons*, 206 F.3d 392 (4th Cir., 2000).
- University of Michigan. Standard Practice Guide 601.16, Policy and Guidelines Regarding Electronic Access to Potentially Offensive Material, July 10, 1997. <<http://www.umich.edu/~policies/offensive-material-60116.html>>, last visited July 2, 2002.
- University of South Carolina. IT 2.15, Harassing or Obscene Telephone Calls or Electronic Messages, March 6, 2002. <<http://www.sc.edu/policies/it215.html>>, and ACAE 7.01, Computer and Network Access and Use, February 1, 1995. <<http://www.sc.edu/policies/acad701.html>>, last visited July 2, 2002.
- University of Southern California. General Policies Regarding the Electronic Communication Infrastructure at the University of Southern California. <<http://www.usc.edu/isd/policies/general/#response>>, last visited July 2, 2002.
- Urofsky v. Allen*, 995 F.Supp. 634 (E.D. Va., 1998), reversed sub nom. *Urofsky v. Gilmore*, 216 F.3d 401 (2000) (en banc), cert. denied, 531 U.S. 1070 (2001).
- Wilborn, S. Elizabeth. "Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace." *Georgia Law Review* 32 (Spring 1998): 825-87.

Copyright of Journal of Labor Research is the property of Transaction Publishers and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.