

## The Privacy Project

# Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace

---

*Employers should have detailed, understandable and fair computer, e-mail and Internet usage policies impartially administered*

---

The evil that men do lives after them;

The good is oft interred with their bones;

—William Shakespeare, *Julius Caesar*, Act III, scene 2

I have come to believe that if anything will bring about the downfall of a company, or maybe even a country, it is blind copies of e-mails that should never have been sent in the first place.

—Michael Eisner (commenting to the graduating class at the University of Southern California)

I suggested deleting some language that might suggest we have concluded the release is misleading.

—E-mail sent by Nancy Temple, in-house counsel for Arthur Andersen, referring to an e-mail that was central to the jury's decision to convict the accounting firm

---

**By William G. Porter II and  
Michael C. Griffaton**

---

WITH JUST a few clicks of a mouse, an employer may lose valuable trade secrets and confidential information, be liable for violating copyright laws, or be exposed to claims that it permitted a hostile work environment. The pervasive and ubiquitous nature and exponential growth of electronic mail and the Internet highlight the need to monitor the electronic workplace to curb that liability.

Just consider:

- The number of e-mail users increased from 8 million in 1991 to 108 million in 2000.<sup>1</sup> In 2000, 40 million employees exchanged more than 60 billion messages daily.<sup>2</sup>

- According to a 1999 study by the

*IADC member William G. Porter II is a senior partner at Vorys, Sater, Seymour and Pease LLP in its Columbus, Ohio, office, where he concentrates his trial practice in business and employment disputes. He is a graduate of Amherst College (1978) and Case Western Reserve University School of Law (1984).*

*Michael C. Griffaton is an associate in the same firm and concentrates in employment law. He is a graduate of Ohio Wesleyan University (1990) and Case Western Reserve University School of Law (1993).*

American Management Association, at least 50 percent of all workplace Internet activity is not business-related.<sup>3</sup>

- A study by the ePolicy Institute found that 85 percent of employees admit to recreational surfing at work.<sup>4</sup> Seventy percent of employees admitted to receiving or sending adult-oriented personal e-mails at work, while 60 percent admitted to exchanging e-mail that could be considered racist, sexist or otherwise “politically in-

---

1. Edward Morawski, *The Internet Around the World: Rising to the Challenge* (Spring 2001) (online at [http://www.angusreid.com/pdf/publicat/fow\\_art.pdf](http://www.angusreid.com/pdf/publicat/fow_art.pdf)).

2. Jay P. Kesan, *Cyber-Working or Cyber-Shirking: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 289 (2002).

3. Samuel Greengard, *The High Cost of Cyber-slacking*, 79 PERSONNEL J. 2224 (December 1, 2000).

4. Elron Software, *1999 Email Abuse Study* (online at [www.elronsw.com/pdf/1999\\_Email\\_Study.pdf](http://www.elronsw.com/pdf/1999_Email_Study.pdf)). See also *2001 Electronic Policies and Practices Survey*, available at [www.epolicyinstitute.com/survey/index.html](http://www.epolicyinstitute.com/survey/index.html)

correct.” Most traffic to Internet pornographic sites occurs during regular business hours, probably because Internet connections usually are faster in the workplace.

Companies have taken note of these statistics and have adopted e-mail and Internet usage policies that may contain provisions for continuous or random monitoring of usage. The ePolicy Institute study reports that 77 percent of employers monitor employees’ e-mail and Internet use. In fact, 10 percent of workers with e-mail/Internet access (about 14 million people) are under continuous online surveillance.<sup>5</sup> About two thirds of employers have disciplined or terminated employees for violating electronic usage policies.<sup>6</sup>

Employers give several reasons for monitoring. Generally, they wish to maintain their professional reputation and image. They also are concerned with employee productivity and business efficiency, as “cyberslacking accounts for 30 to 40 percent of lost worker productivity.”<sup>7</sup> With respect to legal liability, one commentator has stated, “Via the recent expansion of the strict liability doctrine of respondeat superior, an employee may be held strictly liable for the foreseeable torts and crimes of employees.”<sup>8</sup> Therefore, monitoring may assist employers in preventing and discouraging sexual or other illegal workplace harassment, defamation, copyright violations from the illegal downloading of software, music and movies, and the deliberate or inadvertent disclosure of trade secrets and other confidential infor-

mation. The ePolicy Institute study showed that 68 percent of employers that monitor cite legal liability as their primary reason.

No federal or state statute currently prohibits employers from monitoring their electronic workplace. The federal Electronic Communications Privacy Act and similar state laws provide some limitations, but these limitations can be overcome in the workplace through various exceptions in the statutes.<sup>9</sup> The federal act prohibits the interception of electronic communications such as e-mail. It defines “interception” to mean the “contemporaneous acquisition of the communication,” so an interception takes place only when an individual sends an e-mail and a third party is able to obtain a copy of the transmission at the time it is sent.

In reality, however, the act provides employees little protection from the monitoring of their workplace electronic communications. It does not apply to e-mails in their “stored” state. This means that employers can freely obtain copies of e-mails from a network computer or the employee’s hard drive without violating the act. Even when the employer intercepts electronic communications, monitoring is permitted when done in the “ordinary course of business” or when the employee has “consented” to it.

Moreover, few states (among them, Delaware and Connecticut) even require that employers notify their employees of monitoring.<sup>10</sup>

As a general matter, employees in the private sector have no reasonable expecta-

5. *14 Million U.S. Workers under Continuous Online Surveillance*, July 9, 2001 (online at [www.privacyfoundation.org/resources/14million.asp](http://www.privacyfoundation.org/resources/14million.asp)).

6. Greengard, *supra* note 3.

7. Russell J. McEwan & David Fish, *Privacy in the Workplace*, 23 N.J. LAW. 20 (February 2002), citing *Workers Surf at Your Own Risk*, Business week.com, June 12, 2000.

8. Kesan, *supra* note 2, at 311, citing John Edward Davidson, *Reconciling the Tension Between Employer Liability and Employee Privacy*, 8 GEO. MASON U. CIV. RTS. L.J. 145, 147 (1997).

9. 18 U.S.C. § 2510 (2002). For an overview of the Electronic Communications Privacy Act, see Kesan, *supra* note 2, at 295-301. See also N.J. STAT.

ANN. 2A:156A-1 *et seq.* (2002); N.Y. PENAL LAW 250.00 *et seq.* (2002); 18 PA. CONS. STAT. ANN. 5701 *et seq.* (2002).

10. See DEL. CODE ANN. tit. 19, § 705 (2002) (“No employer . . . shall monitor or otherwise intercept any . . . electronic mail or transmission, or Internet access or usage of or by a Delaware employee unless the employer either: (1) provides an electronic notice of such monitoring or intercepting policies or activities to the employee at least once during each day the employee accesses the employer provided E-mail or Internet access services; or (2) has first given a one-time notice to the employee of such monitoring or intercepting activity or policies.”) See also CONN. GEN. STAT. § 31-48d (2002) (“each employer who engages in any type of elec-

tion of privacy in their workplace e-mail and Internet usage that otherwise would abrogate the employer's right to monitor that usage. In fact, courts almost expect that employers will engage in some form of monitoring. As the Seventh Circuit explained in *Muick v. Glenayre Electronics*:

The laptops were [the employer's] property and it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions; but the abuse of access to workplace computers is so common (workers being prone to use them as medium of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that failure to do so might well be thought irresponsible.<sup>11</sup>

E-mail and Internet privacy issues were addressed in the *Defense Counsel Journal* in 2000 by Hall Adams III, Suzanne M. Scheuing and Stacey A. Feeley in *E-Mail Monitoring in the Workplace: The Good, the Bad and the Ugly*.<sup>12</sup> Their paper addressed the central issue of whether an employer can legally monitor employee e-mails and Internet usage without violating employees' privacy or some other state or federal law. The answer to that question was essentially, yes; the courts have consistently rejected claims that e-mail and Internet monitoring represents and invasion of privacy.

This article surveys the flip side of the employer's right to monitor: an employer's liability for actually acquiring information through electronic monitoring, having that information and potentially acting—or failing to act—on that information. In many respects, this delves into uncharted areas of cyberlaw, as the courts are just beginning to explore what liability, if any, employers may have in this arena.

tronic monitoring shall give prior written notice to all employees who may be affected, informing them of the types of monitoring which may occur. Each employer shall post, in a conspicuous place which is readily available for viewing by its employees, a notice concerning the types of electronic monitoring which the employer may engage in. Such posting shall constitute such prior written notice." An employer may conduct monitoring without prior written notice when it has reasonable grounds to believe that

## E-MAIL AND INTERNET USE: EMPLOYEES' CONDUCT AT WORK

Employers have always monitored workplace conduct. In *O'Connor v. Ortega*,<sup>13</sup> for example, the U.S. Supreme Court recognized that employers have legitimate interests in monitoring their employees' work environment.

### A. Sexually Explicit E-mails

In the Seventh Circuit *Muick* case, cited above, federal law enforcement authorities notified Glenayre Electronics, Albert Muick's employer, that they were investigating Muick's dealings with child pornography. At their request, Glenayre seized Muick's workplace computer until the authorities obtained a warrant for it. Muick claimed that Glenayre's actions constituted an unreasonable search and seizure and a violation of his right to privacy.

The court first rejected Muick's claims that the company conducted an illegal search or violated his constitutional rights by cooperating with federal investigators because Glenayre was not acting as a government agent when it turned over the computer to the authorities. Next, the court rejected Muick's right to privacy claim to the computer the employer had furnished for use in the workplace, noting that "Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that Muick might have had and so scotches his claim." The case reinforces the importance of a properly drafted e-mail policy to prevent employees from succeeding in an invasion of privacy claim.

In *Blakey v. Continental Airlines*,<sup>14</sup> Tammy Blakey, Continental Airlines' first

employees are engaged in conduct which violates the law, violates the legal rights of the employer or the employer's employees, or creates a hostile workplace environment, and electronic monitoring may produce evidence of this misconduct.).

11. 280 F.3d 741, 743 (7th Cir. 2002) (parenthetical by the court).

12. 67 DEF. COUNS. J. 32 (2000).

13. 480 U.S. 709, 722 (1987).

14. 751 A.2d 538 (N.J. 2000).

female pilot on the A300 Airbus aircraft, sued Continental in federal court for sexual harassment, discrimination and defamation. During that litigation, a number of Continental pilots posted insulting, defamatory and derogatory remarks about her on the pilot's online computer bulletin board, which was accessible via the Internet by all Continental pilots and crew members through their paid membership in CompuServe. Blakey sued Continental and several coworkers who posted messages on the bulletin board in state court for, among other things, retaliatory sexual harassment.

The New Jersey Supreme Court explained that an employer can be held liable for co-workers' retaliatory harassment if it knew, or should have known, about the harassment but failed to act to stop it, and employers have a duty to take effective measures to stop that harassment in the workplace and settings related to the workplace. Consequently, Continental's liability would depend on whether the on-line forum was such an integral part of the workplace that harassment there should be regarded as a continuation or extension of the pattern of workplace harassment. The case was remanded to the trial court for that determination.

It is notable that the Blakey court did not hold that employers have a duty to monitor private communications of their employees, but it did admonish employers that "it may well be in [their] best interests to adopt a proactive stance when it comes to dealing with co-employee harassment," adding that "the best defense may be a good offense." Effective remedial steps reflecting a lack of tolerance for harassment will be relevant to an employer's affirmative defense that its actions absolve it from all liability for sexual harassment. This case was unusual because the employer did not own the computer network at issue. Where the employer does so, as in most cases, it will be nearly impossible to argue that what occurs on the employer's own

computer network is not an extension of the workplace.

In *Strauss v. Microsoft Corp.*,<sup>15</sup> Karen Strauss, a female employee, sued Microsoft for gender discrimination in failing to promote her, relying in part on sexually related e-mails she received from her supervisor as evidence of gender bias. The e-mails included an advertisement for "mouse balls," a news report on Finland's proposal to institute a "sex holiday," a parody of a play entitled "A Girl's Guide to Condoms," and a message entitled "Alice in Unix Land" that mixed computer language with sexual references. Some of the e-mails were not sent directly to Strauss but by the supervisor to another employee, who, in turn, forwarded them to the rest of the staff.

The U.S. District Court for the Southern District of New York denied Microsoft's motion for summary judgment, concluding that a jury could find pretext for gender discrimination based on the e-mails. Monitoring e-mail could have revealed this conduct and possibly short-circuited the "harassment" of which Strauss complained.

Finally, in *Coniglio v. City of Berwyn*,<sup>16</sup> Susan Coniglio was employed by the City of Berwyn as manager of the its computer department. Allen Zank, the city comptroller, was her direct supervisor. Coniglio alleged that, among other things, Zank regularly viewed pornography on the Internet, in full view of her and other city employees, would print out pornographic pictures and store them in binders in his office, and would invite her into his office and attempt to elicit her reaction to sexually explicit pictures on his computer screen. She testified that the women were sometimes pictured in different sexual positions with creatures resembling medieval gargoyles. Coniglio complained of Zank's behavior, and Zank later terminated her.

She sued, alleging in part that Zank's behavior created a hostile work environment. The U.S. District Court for the Northern District of Illinois denied the city's motion for summary judgment on this claim.

Both *Strauss* and *Coniglio* highlight the importance of e-mail and sexual harass-

15. 814 F.Supp. 1186 (S.D. N.Y. 1993); see also 1995 WL 326492 (S.D. N.Y.).

16. 2000 WL 967989 (N.D. Ill.).

ment policies. Just as calendar “pin-ups” are no longer acceptable in the workplace, on-screen pornographic or sexual images are not acceptable and can be evidence of a hostile work environment. While the employers in those two cases ultimately may prevail at trial, defense of the cases (like most litigation) will be costly in terms of money, time and negative publicity.

While most employees have been trained about improper office behavior—for example, sexual harassment—many do not view e-mail as an avenue for harassment and tend to treat their incoming and outgoing messages more casually than a letter or memo written on company letterhead. In one case that garnered considerable press coverage, Chevron paid female employees \$2.2 million in 1995 to settle a sexual harassment lawsuit from inappropriate e-mail, including “25 Reasons Why Beer is Better than Women,” sent by male employees, including male supervisors.<sup>17</sup>

In *Faragher v. City of Boca Raton* and *Burlington Industries Inc. v. Ellerth*,<sup>18</sup> the U.S. Supreme Court made employers liable for the wrongful action of supervisors that result in adverse employment action, even if the employers were unaware of specific actions involved or taken. If employers fail to take affirmative steps to prevent sexual harassment, they are exposing themselves to potentially larger damage awards. Of course, it is likely that the more an employer monitors its e-mail and Internet usage, the more responsibility the employer will be assessed for its content. As the New Jersey Supreme Court pointed out in *Blakey*, the best defense may be a good offense, and monitoring e-mail and Internet usage may be that “good offense.”

## B. Trade Secrets and Confidential and Proprietary Information

The National Counterintelligence Agency estimates that businesses lost \$44 billion due to economic espionage in one 17-month period.<sup>19</sup> Employers’ greatest risk to their computer security comes not from outside hackers but from current and former employees who deliberately or inadvertently disclose confidential or sensitive information. According to a 2001 survey by Elron Software, more than 40 percent of respondents admitted to receiving company confidential information such as client lists, financial statements and product specifications from “outside their organizations—a 356 percent increase since 1999.”<sup>20</sup> Employees no longer have to photocopy documents surreptitiously; they can simply download reams of data to disk, CD or DVD, or even e-mail the information to a competitor with the click of a mouse.

For example, a former executive of Borland International, a software company, was accused of e-mailing trade secrets to a competitor, which happened to be his new employer, before he quit Borland. Criminal charges were filed, but eventually dropped, and the civil dispute was quietly settled.<sup>21</sup>

In *Frasier v. Nationwide Insurance*,<sup>22</sup> Nationwide searched its file server and located e-mail communications that revealed its employee, Richard Frasier, had e-mailed correspondence critical of Nationwide’s business practices to a competitor. Soon after discovering this, Nationwide terminated Frasier. Frasier sued, alleging that Nationwide had unlawfully intercepted his e-mail communication in violation of

17. Liz Stevens, *Today’s Technology Makes It Easier for Supervisors to Watch Workers*, MILWAUKEE J. SENTINEL, October 6, 1999, at 3.

18. 524 U.S. 775 (1998) and 524 U.S. 742 (1998).

19. James E. Hudson III, *Trade Secret Theft Threatens Everyone with Corporate Economic Espionage Escapades*, HOUSTON BUS. J. TECH. Q., October 1, 1999 (online at <http://www.bizjournals.com/houston/stories/1999/10/04/focus13.html>).

20. Elron Software, *The Year 2001 Corporate*

*Web and Email Study*, 5 (2001) (online at <http://www.elronsoftware.com/pdf/NFOreport.pdf>).

21. See Garry G. Mathiason & Roland M. Juarez, *The Electronic Workplace: An Overview*, CEB CALIF. BUS. L. R. 188, 189 (1995). See *California v. Eubanks*, 927 P.2d 310 (Cal. 1996), as modified and rehearing denied, 1997 Cal. Lexis 1016 (software company paid for services of two computers experts to assist prosecutor).

22. 135 F.Supp.2d 623 (E.D. Pa. 2001).

state and federal wiretap laws and had unlawfully accessed his e-mail from storage in violation of stored communication laws.

The federal district court for the Eastern District of Pennsylvania rejected both contentions, first, because there was no “interception,” and, second, because the employer had lawfully accessed its own equipment and “stored” e-mail to obtain the information.

An electronic monitoring policy may help the employer uncover such activities, perhaps in time to prevent what could be substantial damage to the employer’s business.

### C. Copyright Infringement

Employers also may be needlessly exposed to lawsuits for copyright violations if they permit (or ignore the fact that) employees to receive and/or download software or other materials, such as music, video and graphics files, from e-mail systems or the Internet. Copyright infringement can result in civil and criminal penalties, not to mention adverse publicity. Electronic monitoring is an effective way to minimize that legal exposure for copyright infringement.

Northwestern University, for example, fired Carla Tomina, a secretary who had amassed more than 2,000 MP3 music files on her work computer. While Tomina claimed the files came from her own CD collection, as opposed to those on a website like Napster, the university had been contacted by at least one music copyright holder in connection with unauthorized, downloaded works.<sup>23</sup>

Another company agreed to a \$1 million out-of-court settlement with the Recording Industry of America because the company

had maintained a computer server that employees used specifically for downloading, storing and sharing MP3 files.<sup>24</sup>

### E-MAIL AND INTERNET USE BEYOND THE WORKPLACE

Most electronic monitoring by employers, like the monitoring of employees’ conduct in general, is conducted in the workplace, but employers also monitor and even discipline employees’ off-duty conduct. A common example of monitoring is investigating whether workers’ compensation claimants are in fact working when they claim to be unable to do so. An example of discipline is terminating of an employee who comes to work under the influence of drugs or alcohol. Electronic monitoring expands the employer’s potential range of surveillance and the potential liability for invasion of privacy.

Generally, employees are unsuccessful in claims if the employer can establish a nexus (however somewhat tangential) between the off-duty conduct and the workplace. Some states, such as New York, have made it unlawful to discriminate against employees based on their “legal recreational activities outside work hours, off the employer’s premises and without use of the employer’s equipment or property.” “Recreational activities” means “any lawful, leisure-time activity, for which the employee receives no compensation and which is generally engaged in for recreational purposes, including but not limited to sports, games, hobbies, exercise, reading and the viewing of television, movies or similar material.”<sup>25</sup> Statutes such as this one may limit an employer’s ability to discipline employees for their off-duty, personal e-mail and Internet use.

Many people operate their own websites for personal interests ranging from genealogy to pornography. George and Tracy Miller, for example, were fired from their nursing positions at an Arizona hospital for operating an Internet pornography site showing the Millers engaged in sexual intercourse. They claimed was they operated the site to make money for their children’s

23. Casey Newton, *Downloading MP3’s Gets NU Employee Downsized*, THE SUMMER NORTHWESTERN, July 26, 2001 (online at <http://www.polarity1.com/pcrr3.html>).

24. Benny Evangelista, *Deleting Download: Companies Concerned over Employees’ File-Sharing at Work*, S.F. CHRON., June 3, 2002 (online at <http://www.websense.com/company/news/companynews/02/060302.cfm>).

25. N.Y. LAB. LAW 201-d.

college education. Hospital computer staff alerted hospital administrators that employees were logging onto the site while at work. The hospital initially suspended the Millers pending investigation, and then terminated them, stating that their website created a hostile environment for the hospital's employees. The hospital noted that the Millers had signed a policy statement that provided employees could be discharged for "immoral or indecent conduct" while on or off duty.

The Millers initially filed a charge of discrimination with the Equal Employment Opportunity Commission and received a right-to-sue letter. (It's unclear the protected class into which the Millers would fall.) However, they elected not to pursue the claim and, instead, are now radio talk show hosts.<sup>26</sup>

According to an article in the *Sun-Herald* in North Port, Florida, in March 2001, police officer Daniel Lake was suspended for three days for "conduct unbecoming an officer" for pornography-related activities. The officer, who had a record described as "excellent," was not personally involved with the pornography. Rather, his wife had submitted pornographic images of herself to a voyeuristic website as a birthday present for her husband. While some residents reportedly were opposed to the suspension, police officials were adamant in their belief that they had the right to regulate the personal conduct of a police officer's family.<sup>27</sup>

Bill Owens, a Maryland Home Depot salesman, claimed that his supervisors ignored blatant sexual harassment by a female coworker because he and his wife operated a live sex video streaming site. In May 1999, a female coworker called him "Buck Hunter," his web site pseudonym, asked him for oral sex, exposed her breasts to him and grabbed his crotch in full view of customers. Owens quit because he was afraid of having his secret identity revealed. When he later went back to his supervisor to try to work things out, the supervisor was helpful "until he heard about the site." Owens alleged that his supervisor said that he can protect him from being

grabbed but can't do anything about what people say. Of course, the supervisor is legally incorrect, but Owens ultimately decided not to sue.<sup>28</sup>

Finally, in October 2001, a Georgia police officer sent an e-mail to an online discussion list that advocated "eliminating the entire Arab world" if terrorism continued and suggested that that United States bomb Mecca so that Muslims would be forced to pray "at a crater 25 miles across." The officer had created the discussion list as a forum for law enforcement officers, and the list was not officially tied to any law enforcement agency. The officer's e-mail message, however, carried his professional e-mail signature, which identified him as a police officer. Subscribers to the list complained to the police chief, and the officer agreed to resign.<sup>29</sup>

## PROTECTION UNDER NATIONAL LABOR RELATIONS ACT

### A. Introduction

Employer monitoring of e-mail and Internet usage raises a host of labor law issues. Under Section 8(a)(1) of the National Labor Relations Act (NLRA), employers are prohibited from giving even the impression of surveillance of employees' union activity. As the National Labor Relations Board (NLRB) explained, "Employees should be free to participate in union organizing campaigns without the fear that members of management are peering over their shoulders, taking note of who is in-

26. After Hours, abcNEWS.com, December 9, 1999 (online at [abcnews.go.com/onair/2020/transcripts/2020\\_991209\\_onlineporn\\_trans.html](http://abcnews.go.com/onair/2020/transcripts/2020_991209_onlineporn_trans.html)); *Cyber porn Nurse: "I Feel Like Larry Flynt"* (online at <http://zdnet.com.com/2100-11-515178.html?legacy=zdn>).

27. Elaine Allen-Emrich, *Residents React to Recent City Internet Sex Scandal* (online at <http://www.sun-herald.com/search/search.asp?showarticle=117710>).

28. John Simons, *X-tracurricular Activities*, Business 2.0 (January 2001) (online at [www.business2.com/articles/mag/0,1640,14445,ff.html](http://www.business2.com/articles/mag/0,1640,14445,ff.html)).

29. Erin McClam, *Ga. Cop Asked to Resign for E-mail*, AP Online, October 4, 2001, reported at 2001 WL 28748621.

volved in union activities, and in what particular ways.”<sup>30</sup> Electronic monitoring enables employers to record information about the employees and their activities, often without the employees even realizing it.

Within the past several years, the NLRB General Counsel’s Office has considered several cases involving employer limitations on employee use of company e-mail and computers. The employers generally maintained “no solicitation/no distribution policies” prohibiting dissemination of non-business-related messages through internal e-mail systems. The lead case in this area is *Pratt & Whitney*,<sup>31</sup> in which the general counsel challenged the legality of a business-only e-mail policy. At issue was the use of e-mail by the company’s 2,450 professional and technical employees who worked in one department and communicated extensively via e-mail. The general counsel reasoned that Pratt & Whitney’s policy prohibiting all non-business use of a company’s e-mail and computer system was overbroad and facially unlawful.

Pratt & Whitney’s written policy prohibited the use of computer resources for non-business, unauthorized or personal purposes. However, the policy was not strictly enforced, and employees often violated it. After a union organizing campaign was underway, the employer disciplined several employees who were union activists for sending e-mail messages and downloading union-related information onto the company computer. After finding that the employer violated the NLRA by disparately and discriminatorily enforcing its policy

only against employees sending union messages, the general counsel outlined a new theory, derived from no-solicitation and no-distribution case law, that the mere existence of a business-only policy violates the NLRA—in effect, that a business-only policy was similar to a no-solicitation policy.

In labor law parlance, no-solicitation rules prohibit employees from communicating to fellow employees for various causes, including union organizing. To be lawful, a no-solicitation rule must be non-discriminatory (it cannot apply just to union organizing), and it must apply only to solicitations that take place in work areas during working time. A company may not ban solicitation by employees during non-working time, whether or not it occurs in a work area. No-distribution rules prohibit the distribution of literature on the employer’s premises, and they also must be non-discriminatory. However, a company may lawfully ban distribution of materials in work areas at any time, whether working or non-working, but in most industries, an employer cannot ban distribution by employees in non-work areas.

In the *Pratt & Whitney* opinion, the general counsel first concluded that employee computer workstations were work areas. Next, the opinion noted that the employer’s e-mail system was used as a tool for conversations and that the business-only rule prevented the employees from conversing about the union during their non-working time. Accordingly, this is as unlawful as a no-solicitation rule that bans solicitation during non-working time.

## B. Recent Cases

In an NLRB general counsel case, *TXU Electric*,<sup>32</sup> the employer adopted this e-mail policy:

Internet, Intranet and E-mail are provided by the Company for business-related use. Any personal use by Users must be kept to a minimum (no more than five (5) User I.D.’s per E-mail), must comply with all Company policies, and must not involve sending or storing files which consume large amounts

30. *Flexsteel Indus. Inc.*, 311 NLRB 2547 (1993). For an overview of the union-related issues surrounding e-mail, Internet usage, and electronic monitoring in the workplace, see Frederick D. Rapone Jr., *This Is Not Your Grandfather’s Labor Union—Or Is It? Exercising Section 7 Rights in the Cyberspace Age*, 39 DUQ. L. REV. 657 (2001); Gwynne A. Wilcox, *Section 7 Rights of Employees and Union Access to Employees: Cyberorganizing*, 16 LAB. LAW. 253 (2000).

31. 1998 WL 1112978 (NLRB General Counsel, February 23, 1999).

32. 2001 WL 1792852 (NLRB General Counsel, February 7, 2001).

of computer storage space. Personal E-mail should not exceed one-half (1/2) page in length or contain photographs, video or file attachments. Additionally, sending chain E-mail or non-business related bulk E-mail is prohibited. Users may not use Company resources to create a personal home page, web page, or computer programs.

The union contended that the employer's e-mail unlawfully restricted employees and union representatives from the exercise of their rights under the NLRA. The general counsel disagreed, concluding that the policy was facially lawful because it permitted employees to use the e-mail system for personal use but only limited the length of the message and the number of employees to which a particular e-mail may be sent. The opinion held that the policy narrowly addressed the employer's legitimate business concerns—to forestall significant interference with its use of the e-mail system—while adequately balancing employees' Section 7 rights and the employer's managerial interests.

Such limitations are lawful, according to the general counsel, as there was sufficient evidence demonstrating a substantial business justification that unfettered personal use would impair the effectiveness of the e-mail system significantly. Because there was no restriction on the number of e-mails that employees could send (as opposed to size the e-mail messages), employees still had the opportunity to communicate effectively throughout the bargaining unit.

In *IRIS-USA*,<sup>33</sup> the general counsel upheld a ban on all personal e-mail where the computers were not part of the employees' work area. Because the employees did not use computer or e-mail as part of their regular work, a work area "did not exist for them."

*Sitel Corp.*<sup>34</sup> highlights the fact that employees' right to concerted activity guaranteed by the NLRA applies in both the union and non-union workplace. The e-mail policy in question restricted the use of the employer's computer and e-mail system to work-related purposes. The employees, who were not represented by a union, had regular access to a computer network,

including e-mail and the Internet. An employee named Scully was disciplined after he forwarded an e-mail from a former employee regarding working conditions at Sitel. It was well-known at Sitel among both management and employees that employees commonly used the computer system, the Internet, and e-mail for numerous non-work-related purposes.

Scully won a Pyrrhic victory. The general counsel determined that the company's e-mail policy was unlawfully overbroad and that the company unlawfully disciplined Scully for criticizing the working conditions.<sup>35</sup> The opinion went on, however, to note that the company eventually—and lawfully—discharged Scully for viewing pornographic web sites on his computer. This case highlights the importance of monitoring employee Internet activity.

### C. Observations and Unanswered Questions

The NLRB general counsel's advice memoranda raise, but do not answer, several questions about the scope of the traditional no-solicitation and no-distribution rules. Under the well-established no-distribution rule, an employer can ban distribution of materials in work areas at any time; an employer may not ban solicitation that occurs on non-work time regardless of where the solicitation occurs. If an employee does not have set break times, it is difficult to draw the line between non-work and work time. If the employee sends an e-mail to all fellow employees about working conditions and the employees read the e-

33. 2000 WL 257107 (NLRB General Counsel, February 2, 2000). See also *Emcompass Services Corp.*, 2001 WL 310613 (NLRB General Counsel, January 18, 2001).

34. 2000 WL 33252020 (NLRB General Counsel, October 5, 2000).

35. See also *Timekeeping Sys.*, 323 NLRB 244 (1997) (employee who sent e-mail to other employees critical of company's vacation policy was engaged in "concerted activity," which is protected by the NLRA; company president's termination of employee because employee refused to publicly apologize for sending e-mail was unlawful; employee reinstated with back pay).

mail while at their desks, is that e-mail a “solicitation” or a “distribution”? If an employee with an established break time reads the e-mail in his work area when he is not on break, does the e-mail then become a prohibited distribution and solicitation? What if the employee is on break but is in his work area, is the e-mail a distribution (material read in the work area) or a solicitation (material read on non-work time)? What happens if the employee prints out the e-mail and reads it in the break room?

There are no easy answers to those and the myriad other scenarios that may arise as e-mail use continues to proliferate. At this point, the NLRB general counsel has provided little guidance for employers.

One thing that is clear, as the above cases point out, is that an employer generally cannot discipline an employee because of the content of the employee’s e-mail message. Depending on the scope of the e-mail policy, however, the employer may be able to discipline an employee because the employee violated the e-mail policy, for example, by sending pornographic images or file attachments that are too large, or by sending the e-mail to too many recipients.

### **NAVIGATIONAL AIDS FOR THE ELECTRONIC WORKPLACE**

Once the employer begins to monitor employees’ e-mail and Internet usage, what happens to all the saved e-mails and Internet history logs? How long is that information saved? How long should it be saved? What should the employer do with all the information it has logged through its electronic monitoring efforts?

#### **A. Electronic Discovery**

First and foremost, employers (and employees) must remember that e-mail is not necessarily gone when “deleted.” The informality of e-mail and the mistaken belief that it can be erased easily often result in the creation of evidence that can make or

break a case. Electronic evidence that can be monitored includes not just e-mail and Internet usage, but it also includes computer user files, applications, databases, spreadsheets, network log files, access activities, back-up tapes, data remnants, metadata, and deleted files. Rule 26(a) of the Federal Rules of Civil Procedure requires parties disclose computer-based evidence that they may use to support their claims or defenses, and Rule 34 has been interpreted to mean that electronic documents must be produced in their “native format.”<sup>36</sup>

Employers also must remember that document destruction is not permitted simply because no subpoena has been served or because litigation has not commenced. Some courts do not consider destruction of potential evidence before a lawsuit is filed as spoliation, while others find that a duty to preserve documents arises when a party should reasonably know that litigation is imminent. Some courts presume that document destruction under a company policy is innocent, while others question whether a duty to preserve was triggered regardless of such a policy.

The traditional approach to reducing the legal risk with old e-mail messages is to create written policies that define the “useful life” of different document types and thereby limit the spread of information. Moreover, various state and federal administrative agencies require certain documents to be preserved for periods of time. For example, Title VII of the Civil Rights Act generally requires that any personnel or employment record be preserved for one year after the date the record was made or the undertaking of the personnel action involved, whichever is later. If an employee is involuntarily terminated, such records must be kept for one year following the date of termination.<sup>37</sup>

Hand-in-hand with monitored information is deciding how long to retain it. Current storage media make it easy and inexpensive to save almost everything indefinitely. Of course, this also makes it easy to “forget” that the information is there. The most telling example of docu-

36. *United States v. Microsoft Corp.*, 1998 WL 699028 (D. D.C.).

37. 29 C.F.R. §§ 1602.14; 29 C.F.R. § 1627.3(b).

ment retention and destruction problems is the Arthur Andersen trial resulting from the Enron bankruptcy. The Andersen policy called for the retention of important company documents but the destruction of extraneous records. Andersen lawyer Nancy Temple sent an e-mail on October 12, just five days before the Securities and Exchange Commission opened an informal inquiry into Enron, reminding workers of the policy.<sup>38</sup> David Duncan, the former Andersen lead auditor for Enron and the government's chief witness in the case, testified during the trial that he "obstructed justice" by "instruct[ing] people on the team to follow the document retention policy, which I knew would result in the destruction of documents."<sup>39</sup>

Destruction of documents can be costly in more ways than one. In one case, a court fined Prudential Insurance \$1 million for its "haphazard and uncoordinated approach to document retention" in face of a court order requiring retention, even though there was no proof that Prudential intended to thwart discovery. The court also instructed the jury that it could draw an adverse inference that destroyed documents were relevant and unfavorable to Prudential.<sup>40</sup>

Courts have upheld requests for production of documents that required companies to spend thousands, and even tens of thousands, of dollars to retrieve "deleted" information or information stored on back-up tapes and servers. In one case, the defendants were ordered to bear the cost of searching through 30 million pages of e-mail despite their estimate that it would cost between \$50,000 and \$70,000. It is notable that the court stated, "If a party

chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk."<sup>41</sup>

Litigation is costly in any event. Electronic discovery battles can be even more costly.<sup>42</sup>

## B. Electronic Monitoring Policies

Employers considering monitoring their electronic workplace are well advised to create a monitoring policy detailing the types of monitoring used and why, explaining what kinds of e-mail or Internet usage is allowed and what is not. Included in the policy should be the actions that will be taken if the policy is violated. Employers must notify employees of the monitoring and should ensure that the employees return a signed acknowledgment of their understanding of the policy and of the ramifications for violating it.

Like other policies, the electronic monitoring policy should be re-evaluated periodically, and any revisions should be redistributed, signed and returned by the employees. Employers also should update their anti-harassment policies to include specific references to inappropriate e-mail and Internet usage. Finally, employers must train and periodically remind managers and employees of the policy.<sup>43</sup>

Employers can take computer monitoring a step further than merely looking through computer files; they can use the computer itself to help by employing a plethora of software designed specifically to monitor computer activity. One manufacturer of monitoring software even claims to be able to detect potential workplace violence from monitoring employees' e-mail.<sup>44</sup>

38. Jonathan Weil et al., *Andersen Win Lifts U.S. Enron Case*, WALL ST. J. June 17, 2002, at A1.

39. Milton Lawson, *Duncan Testifies about Shredding*, WASH. TIMES, May 14, 2002 (online at <http://www.washtimes.com/upi-breaking/14052002-023744-292lr.htm>).

40. *In re Prudential Ins. Co. Sales Practices Litig.*, 169 F.R.D. 598, 617 (D. N.J. 1997).

41. *In re Brand Name Prescription Drugs Anti-trust Litig.*, 1995 U.S. Dist. Lexis 8281 (N.D. Ill.).

42. See Jason Krause, *Electronic Documents Are Vital to Building a Case, So Don't Get Papered*

*Over*, ABA J. July 2002, at 49; Kevin L. Carr, *Electronic Data: The Legal and Practical Aspects of Retrieving Electronic Data in Discovery*, ABA Labor and Employment Law Section (Midyear Meeting, March 2001).

43. See Torianne Florentino, *Employee Privacy in the Ever-Evolving Workplace*, 701 PRAC. L. INST. 679, 702-704 (2002).

44. See John C. Dvorak, *Monitoring the Emotional State*, Forbes.com, May 5, 2001 (online at [www.forbes.com/2001/05/14/0514dvorak.html](http://www.forbes.com/2001/05/14/0514dvorak.html) (discussing Stroz Associates)).

Monitoring software generally falls into the following categories:

- **Blocking software.** This type of software filters virtually anything on the Internet that the employer deems inappropriate for employees to access while at work. When employees type in questionable words or search inappropriate sites, which have been predetermined by the employer, not only are they prevented from entering, but they may be directed automatically to the company's electronic communications policy. The software also can alert employers when an off-limits site is visited. The main features of this software include [www.cybersitter.com](http://www.cybersitter.com), [www.net.shepherd.com](http://www.net.shepherd.com), [www.xstop.com](http://www.xstop.com), and [www.surfwatch.com](http://www.surfwatch.com).

- **Direct surveillance.** This software takes a picture of an employee's screen at periodic intervals, which enables the employer to see the sites employees are visiting or the messages they are e-mailing. An example is [www.spectersoft.com](http://www.spectersoft.com).

- **Flagging.** This software not only monitors employees' Internet use but also screens their e-mail for potentially offensive or inappropriate messages. This software scans employee e-mails for questionable keywords pre-determined by the employer. For example, an employer concerned with the theft of its trade secrets can list the names of its primary competitors as keywords. This software also can automatically e-mail "flagged" messages to a company representative. An example is [www.cybersitter.com](http://www.cybersitter.com).

- **Keystroke logging.** This software maintains a record of keystrokes and tracks

computer idle time. This software can even recreate "deleted" documents because the keystrokes are logged and stored even if deleted. See, for example, [www.adavi.com](http://www.adavi.com). The Program Investigator from [www.winwhatwhere.com](http://www.winwhatwhere.com) also monitors every instant message.

Electronic usage policies are effective only if utilized consistently, regularly and fairly. To reduce legal risk effectively, employers must enforce these policies consistently, without imposing undue burdens on employees or its computer staff. Ideally, the system must support time- and event-based destruction of old messages and must allow a company to halt scheduled deletion of messages selectively in order to respond to preservation orders and discovery requests. Finally, the electronic monitoring policy must be coordinated with other records management systems so that computer administrators can apply retention rules to different types of records.

## CONCLUSION

- Dow Chemical fired 74 employees, including executives, and punished 435 others for distributing and viewing sexually explicit and graphically violent materials via company e-mail in 2000. One worker commented that he didn't think the e-mail "jokes" he sent were offensive because "most of the people in his department were either receiving or sending similar messages."<sup>45</sup>

- Xerox fired more than 40 employees for wasting up to eight hours a day surfing pornographic websites in 1999.<sup>46</sup>

The U.S. Supreme Court has held that "an employer can be liable [for workplace co=worker harassment] where its own negligence is a cause of the harassment. An employer is negligent with respect to sexual harassment if it knew of or should have known about the conduct and failed to stop it. Negligence sets a minimum standard for employer liability under Title VII."<sup>47</sup>

Employers therefore may be considered negligent if they do not monitor their electronic workplace, just like they may be

45. Brenda Rios, *Dow's Audit of Workers' E-mail Ends in Firings*, DETROIT FREE PRESS, July 27, 2000 (online at [www.freep.com/money/business/doww27\\_20000727.htm](http://www.freep.com/money/business/doww27_20000727.htm)); *Dow Chemical Fires 50 over E-Mail Abuse*, USA TODAY, July 28, 2000 (online at [www.usatoday.com/life/cyber/tech/cti298.htm](http://www.usatoday.com/life/cyber/tech/cti298.htm)); *Dow Chemical Fires Another 24 over E-Mail*, USA TODAY, September 14, 2000 (online at [www.usatoday.com/life/cyber/tech/cti530.htm](http://www.usatoday.com/life/cyber/tech/cti530.htm)).

46. Bloomberg News, *Xerox Fires 40 for Online Pornography on Clock* (online at <http://news.com.com/2102-1001-231058.html?legacy=cnet>).

47. *Burlington Indus. v. Ellerth*, 524 U.S. 742, 758-59 (1998).

considered negligent for failing to monitor their physical workplace. Employers may avail themselves of the affirmative defense if they take prompt and effective remedial action to end harassment once they know or should have known of it. If the employer fails to do so, "the combined knowledge and inaction may be seen to demonstrate negligence."<sup>48</sup>

Another reason to monitor employee e-mail and Internet usage is to gather support for an after-acquired evidence defense to an adverse employment action. This defense generally enables an employer to avoid some (or even all) liability where it could show, after terminating an employee even for unlawful reasons, that it learned the employee previously had engaged in conduct that, if discovered, would have led to termination. With respect to federal anti-discrimination laws, the Supreme Court has held that after-acquired evidence cannot operate to bar all relief, but it can limit damages award and generally will render reinstatement and front pay inappropriate.<sup>49</sup>

For example, suppose a terminated employee sues for discrimination. After culling through the employee's e-mails, the employer learns that the employee was sending confidential information to com-

petitors or pornographic e-mails to co-workers, both of which are violations of the company policies. The employer then raises the after-acquired evidence defense in reliance on this information. To be effective, the employer's electronic communications policy must specifically prohibit the usage that would subject the employee to discipline.

It is still too early to draw conclusions about what course the courts will chart on monitoring the electronic workplace. By tracking and monitoring employee usage, the employer may be storing information that might later be used against it. By not monitoring, given the prevailing notion that most workers engage in at least some form of personal use of their workplace computers, employers may be complicit in maintaining a hostile work environment.

---

48. *Faragher v. City of Boca Raton*, 524 U.S. 775, 789 (1998).

49. *See McKenna v. Nashville Banner Pub. Co.*, 513 U.S. 352, 363 (1995) ("Where an employer seeks to rely upon after-acquired evidence of wrongdoing, it must first establish that the wrongdoing was of such severity that the employee in fact would have been terminated on those grounds alone if the employer had known of it at the time of the discharge.").

