EMPLOYEE USE OF THE INTERNET: WHERE VOYAGE IS FORBIDDEN

Warning: Using your e-mail at work for personal use could be hazardous to your employment status.[1]

The technological developments of recent years have been both a blessing and a curse for corporate America. While new advances have helped to improve corporate efficiency, productivity and growth, such technology also has created numerous potential liability concerns. The Internet has served as a primary source of these concerns. As corporations increase employee access to the Internet, this entry to information increases the potential for employee computer abuse. In sum, the enormous workplace potential of the Internet and e-mail is being undermined by employees who can, with a click of a mouse, distribute confidential records worldwide in a matter of minutes, peruse pornography over the Internet from their office computers, or send sexually harassing messages via e-mail, chat rooms or newsgroups. Understandably, the overwhelming response from employers has been to monitor their employees' activities more closely now than ever before because of the loss of work time productivity and the liability often

---

*Dr. Elizabeth A. Cameron, Associate Professor of Business Administration at Alma College, Alma, MI, and Dawn R. Swink, Assistant Professor for the Department of Legal Studies in Business, University of St. Thomas, St. Paul, MN.

[1] Numerous law reviews and comments have been written on different areas of electronic monitoring in the employment context. *See e.g.*, Sarah DiLuzio, *Workplace E-Mail: It's Not as Private as You Might Think*, 25 DEL. J. CORP. L. 741 (2000); Amy Rogers, *You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace*, 5.1 J. TECH. L. & POL'Y 1, (Spring 2000); Scott A. Sundstrom, Note, *You've Got Mail! (And the Government Knows It): Applying the Fourth Amendment to Workplace E-Mail Monitoring*, 73 N.Y.U.L. Rev. 2064 (Dec. 1998); Dan McIntosh, Comment, *e-monitoring@workplace.com: The Future of Communication Privacy in the Minnesota Private-Sector Workplace*, 23 HAMLINE L. REV. 539 (Spring

created from the paper trail of e-mails. Yet many employees are not aware of these extensive practices. Not only is it possible for an employer to legally access an employee's computer, e-mail and files from remote sites, sophisticated technology allows an employer to obtain a printout of every key that is pressed by the employee during the workday![2] This means that even e-mail messages that an employee deleted from the computer can be retrieved by the employer or other third parties. For many American employees, such monitoring practices raise issues of invasion of privacy. For government employees, the concern lies with violations of Due Process under the Fifth[3] and Fourteenth[4] Amendments and unreasonable searches and seizures under the Fourth Amendment.[5]

This article explores the rights and duties of employers and employees regarding an employee's use of the Internet while at work. First, it examines an employee's use of the Internet for personal endeavors such as personal e-mail, online personal shopping, employment searches, viewing pornography, banking and other non-work related activities. Second, it highlights the extent of employer monitoring. Third, it discusses potential employer legal liabilities for an employee's online activities and related reasons for monitoring. Fourth, it details recent cases of an employee's right to privacy and an

---

2000); Caitlin Garvey, Comment: *The New Corporate Dilemma: Avoiding Liability in the Age of Internet Technology,* 25 DAYTON L. REV. 133 (Fall 1999).

[2] *Employee Monitoring—How Far Will It Go?* IDAHO EMP.L.LETTER, June 2000, LEXIS, News Library, Emplaw file (two programs currently on the market to monitor an employer's every keystroke are "Investigator 2.0," from Win What Where and "Silent Watch.") Investigator 2.0 gathers details on every keystroke touched, every menu item clicked, all the entries into a chat room, every instant message sent, and all e-commerce transactions. It then invisibly e-mails a detailed report to the employee's boss. *See* Stuart Glascock, *Stealth Software Rankles Privacy Advocates*, TECHWEB NEWS, Sept. 17, 1999.

[3] U.S. CONST. amend. V.

[4] U.S. CONST. amend. XIV.

[5] U.S. CONST. amend. IV.

employer's right to performance of work-related tasks; and finally, it discusses current policies and monitoring devices used by employers.

I. EMPLOYEE ABUSES OF THE "SYSTEM"

Clearly there are an increasing number of cases involving employee abuse of both e-mail and the Internet. In 1995, Chevron Corporation settled a $2.2 million lawsuit brought when its employees were offended by an e-mail entitled, "25 Reasons Why Beer is Better Than Women."[6] Morgan Stanley, a large Wall Street brokerage, was sued for $70 million by workers over racist jokes that appeared on the company's e-mail system.[7] In 1999, Xerox Corporation fired 40 employees for spending work time—in some cases up to eight hours a day—sending or storing pornographic e-mail or looking at forbidden web sites. A month later, The New York Times fired 22 people at a pension office in Norfolk, Virginia, for passing around potentially offensive e-mails, including some that a spokeswoman said included sex jokes and pornographic images.[8] In 2000, Dow Chemical Company at its Midland, Michigan, plant fired 50 employees and disciplined 200 others for abuse of e-mail. The abuse included off-color jokes, pictures of naked women, depiction of sex acts and violent images.[9] Two months later at its Freeport,

---

[6] *See* Chen Bin, *Preventing Internet Misuse in the Office*, BUSINESS TIMES SINGAPORE, June 18, 2001, at SS13, Say IT.

[7] *See* Dana Hawkins, *Who's Watching Now? Hassled by Lawsuits, Firms Probe Workers' Privacy,* U.S. NEWS & WORLD REPORT, Sept. 15, 1997, at 56.

[8] *Id.*

[9] Associated Press, *Dow Fires 50 Workers Over E-Mail Abuses*, N.Y. TIMES, July 28, 2000, at A-18. Dow has been sharply criticized for taking such an aggressive approach in response to one complaint over an e-mail attachment, particularly since in its blue-collar tradition, dirty jokes and tasteless pictures had always been in the Dow workplace and management had never taken action before. "Companies do not generally terminate employees on the first abuse. Most start with warnings," says David Lewin, a professor of human resources at UCLA. *Id.* Moreover, the company's monitoring technique did not seem "fair" either. It took a "snapshot" of its entire network on May 9th. Those employees who had exchanged a dirty e-mail on that particular day were caught and

Texas, manufacturing plant, Dow fired 24 workers and disciplined an additional 235 employees for the same misconduct.[10] Other major corporations have been impacted as well. Employees at Apple, AT&T and IBM were discovered to have visited the Penthouse web site 12,823 times in one month.[11]

The list continues to grow. With an estimated total online workforce in the United States of 40 million people,[12] it is foreseeable that employees will not always be devoting their workplace time to their employers' business. How much time do employees spend surfing the net or answering e-mail when they are supposed to be working?

Surveys have shown that ninety percent of employees with access to the Internet look at non-work-related Internet sites at least once a day,[13] ninety percent receive non-work related e-mail[14] and eighty-four percent send non-work related e-mail.[15] If the employees only checked their e-mail once a day, it might not be so bad. In a different survey of one thousand people, eleven percent said they checked their e-mail up to *ten times* a day.[16] In a recent article by Websense, Inc., the company identified reports finding that during the

---

disciplined, even if they had never sent or received such an e-mail at work before. Others, who may have exchanged hundreds of dirty e-mails either before or after that frozen moment, were not caught and were not disciplined. *Id*.

[10] Todd R. Weiss, *Dow Fires More Employees Over Inappropriate E-mails*, COMPUTERWORLD, Sept. 19, 2000 http://www.cnn.com/2000/Tech/computing/09/19/dowfiring.idg/index.html (*last visited* Oct. 30, 2001).

[11] Jon Tevlin, *Cyberloafing*, MINNEAPOLIS STAR TRIBUNE, Feb. 23, 1998, at 6, Tech Today.

[12] *See Employers Monitor a Third of Online Workforce*, U.S.A. TODAY, Aug. 13, 2001, at http://www.usatoday.com/news/nation/2001/07/10/internet-monitor.htm. (citing Nielsen/NetRatings).

[13] Dyland Loeb McClain, *I'll Be Right With You, Boss, as Soon as I Finish My Shopping*, N.Y. TIMES, Jan. 10, 2001, at G-1.

[14] *Id.*

[15] *Id.*

[16] *See* Lisa Fickenscher, *The Side Effects of Surfing on the Job*, N.Y. TIMES, May 21, 2000, at 3-12 (emphasis added).

workday hours of nine-to-five, seventy- percent of all Internet porn access[17] and sixty percent of online purchases occur.[18] Charles Schwab has revealed that ninety-two percent of its customers who buy or sell mutual funds will do so during the nine-to-five work hours.[19] It has been estimated that the average employee with Internet access spends approximately six hours per week online.[20] Aside from viewing pornography, shopping online and checking investments and the news,[21] the following categories are the most popular Internet activities for employees: banking, 34%; arranging child care, 16%; shopping for groceries, 12%; researching health care, 12%; making appointments, 7% and planning social events, 6%.[22]

Most office employees falsely assume that the e-mail messages they send and receive are private and confidential. In fact, e-mail sent or received via the employer's e-mail system is increasingly subject to company control and monitoring. The motivation to monitor employees stems from potential liability that employers face for the contents of employee e-mail messages and employee activities on the Internet; however, this is

---

[17] WEBSENSE, at http://www.netpart.com/index2.cfm, (citing SexTracker).
[18] *Id*. (citing Nielsen/NetRatings).
[19] *Companies Are Turning to HR for Control of Workplace Internet Abuse*, Human Resource Management Department Report, Jan. 2000, *at* LEXIS, News Library, Emplaw file.
[20] *Id. But see* McClain, *supra* at 13 (claiming the average time is one hour and twenty minutes per day). *See also* Anne Colden, *Web-Savvy Workers Giving Employers Pause: Companies Need Policy to Define Acceptable Use*, DENVER POST, Nov. 5, 2000 (citing a 2000 Vault.com survey showing 13% of employees are surfing for more than 2 hours a day at the office).
[21] *See* Mark Harrington, *At Work, Surf City: Poll Shows Employees' Internet Habits*, NEWSDAY, April 7, 2000, at A06 (citing a Nielsen national study stating that news sites reach 35.5 percent more users at work than at home). A recent Vault.com survey showed 72% of employees surveyed read the news online at work. *See* Anne Calden, *supra* at 20.
[22] Harrington, *supra* at 21. A 2000 Vault.com survey of 451 employees found 45% used the Internet to perform travel planning; 40% shopped, 37% job searched, 34% checked their stocks, 26% engaged in instant messaging, 13% downloaded music and 11% played games on their computers at work. *See* Anne Colden, *supra* at 20.

enhanced by the relatively low cost[23] and ease provided by advanced technology. Employers assert that monitoring employees is justified since the computer system is owned and operated by the company, and that the employee should be performing tasks related to the job.

Employees, on the other hand, believe that if an employer has given them a computer and a password, there is an expectation of privacy in personal communications. In addition, while the majority of employees agree that it would be "highly unethical" to sabotage the computer system of an employer, only a small percentage believe that web surfing or shopping or even using personal e-mail while at work is unethical.[24]

II. MONITORING DATA

A survey of 301 companies in 1993 revealed that approximately twenty-one percent of employers searched their employees' computer files, voice mail, and e-mail or other networking communications systems. Of these, almost one-third of these companies did not warn their employees of this practice.[25] Surprisingly, as of 1998, few companies had specific guidelines or company policies on e-mail and Internet usage in the workplace.[26] Today, in part because of the fear of legal liability for hostile work environments or other illegal activities such as online defamation and, in part, to protect proprietary property

---

[23] Worldwide sales of employee-monitoring systems are estimated at $140 million a year, or about $5.25 per monitored employee per year, according to the Privacy Foundation. *See More Employers Monitoring Workers' E-Mail, Web Use*, THE INDUSTRY STANDARD, July 9, 2001, *at* http://www.thestandard.com/article/0,1902,277766,00.html.

[24] *See* Vivian Marino, *Diary: Confessions of Workers At Play on the Computer*, N.Y. TIMES, July 15, 2001, at 3-10.

[25] Charles Piller, *Bosses With X-Ray Eyes*, MACWORLD, July1993, at 118, 122.

[26] *See* Leyla Kokmen, *Firms E-Mull Computer Policies: Employees' Personal Use a Concern*, DENVER POST, Mar. 22, 1999, at E-01 (citing a 1998 International Data Corporation survey showing that 60 percent of 172 companies interviewed had no policies on employee usage of e-mail or Internet).

and measure productivity, many employers are monitoring their employees on a much larger scale.

For example, in *Vega-Rodriguez v. Puerto Rico Telephone Co.*,[27] Vega and others were employed as security operators for the Puerto Rico Telephone Company (PRTC). PRTC installed a video surveillance system in the open workspace in the center. Three cameras surveyed the workspace and a fourth observed traffic in the main entrance. The surveillance was only visual and did not cover the rest area.[28] The cameras operated all day, every day, and recorded every action taken in its preview. The employees complained to management that the system had no business purpose engaging in this activity and was prying into employee behavior.[29] Management did not respond, and a complaint was filed with Puerto Rico's federal district court. The employees argued that the video cameras violated their Fourth Amendment protection against unreasonable searches and invaded their constitutional rights to privacy and First Amendment rights.[30]

However, the Court of Appeals unanimously held that PRTC did not violate the plaintiffs' Fourth Amendment protection when the video cameras were installed in common work areas. The Court stated that the employees did not have an objectively reasonable expectation of privacy in the open areas where they worked.[31]

According to a recent survey by the American Management Association,[32] 77.7 percent of U.S. corporations monitor some form of their employees' communications,

---

[27] 110 F.3d 174 (1st Cir. 1997).
[28] *Id*. at 176.
[29] *Id*. at 176-77.
[30] *Id*. at 177.
[31] *Id*. at 184.
[32] *See* 2001 American Management Association Survey *Workplace Monitoring and Surveillance: Policies and Practices, Summary of Key Finding*, April 2001, http://www.amanet.org/research.

including their phone calls, computer files, e-mail and Internet connections.[33] Although the monitoring of telephone usage and computer files has increased in recent years, the increase is not nearly as great as the increase in monitoring e-mail and Internet usage. In 2001, the AMA reported that of 1627 corporate responses to its survey, only 19.7% said they reviewed telephone records and voice mail messages.[34] This figure is up only slightly from 1997 when corporations reported telephone and voice mail monitoring of 15.7%. However, employer storage and review of e-mail has increased dramatically during the same time period. In 1997 only 14.9% of the respondents said they monitored e-mail. By 2001 that figure rose to 46.5%. Monitoring of Internet connections was even greater; 62.8% of employers reported that they monitored employee Internet connections.[35]

III. WHY MONITOR?

Employers may have legitimate business interests that justify some type of employee monitoring. These business interests include: statutory compliance, performance review, productivity measures, security concerns, and perhaps most importantly, legal liability for what transpires in cyberspace on company computers and on company time.

In regulated industries, electronic recording and storage may be considered part of a company's "due diligence" in keeping adequate records and files pursuant to statutory

---

[33] *Id*. A study conducted by the Workplace Surveillance Project of the Privacy Foundation estimates 14 million employees are continually under surveillance using commercially available software. *Employers Monitor a Third of Online Workforce*, *supra* at 12. *See also* ComputerWorld, *More Employers Monitoring Workers' E-Mail, Web Use*, THE INDUSTRY STANDARD, July 9, 2001 *at* http://www.thestandard.com/articles (estimating that the number of employees under surveillance worldwide is about 27 million) (citing Privacy Foundation).

[34] 2001 AMA Survey, *supra* at 32.

mandate.[36] In addition, taping telemarketing activities gives both the company and the consumer some degree of legal protection.

In those businesses offering customer service or concentrating on customer relations, employers utilize monitoring for performance evaluation and to assist in the improvement of an employee's job performance. Most frequently this type of monitoring involves the taping of telephone calls or reviewing telephone logs.[37] However, such surveillance can be used to measure an employee's work output as well.

Employers are becoming increasingly concerned about the loss of productivity that results from allowing employees Internet and e-mail access. And they should be. ZDNet reports that when the web broadcast the Starr report and Clinton grand jury video, companies lost $450 million in employee productivity as workers tuned in.[38] At least one projection during the 2001 NCAA basketball tournament was that employers lost $400 million in productivity because of employees checking tournament scores on the web.[39]

Tiberino v. Spokane County[40] is an example of the impact on productivity an employer faces when an employee misuses the Internet for personal purposes. Gina Tiberino was hired as a secretary in the special assault unit of the prosecutor's office for Spokane County, Washington. She was employed less than three months when other employees complained that Tiberino was sending excessive and sometimes vulgar personal e-mail

---

[35] *See id*. This figure is up from 54.1% in 2000. No questions concerning Internet monitoring were included in the AMA survey prior to the year 2000.
[36] *See id*. (citing 50.1% of respondents indicating that legal compliance is a high priority concern).
[37] *Id.*
[38] *See Web Filtering Packages Stem Rising Tide of Employee Internet Abuse*, IOMA, Jan. 2000, LEXIS, News Library, Emplaw file.
[39] Greg Auman, *Sites to See—If the Boss is Not Looking,* ST. PETERSBURG TIMES, Mar. 16, 2001 (citing a projection by Websense, Inc.).
[40] 13 P.3d 1104 (Wash. App. 2000).

messages on the Internet. An administrator checked Tiberino's sent mail file and found "that approximately 214 messages had been sent. Of those messages, 200 were sent via the Internet to her sister and mother.[41] Approximately 10 to 15 of these messages appeared to be work related." [42] Tiberino was later terminated for poor work performance and for sending excessive personal e-mail messages. The prosecutor's office printed all e-mails written by Tiberino while employed. At that time, the sent mail folder contained 551 e-mails sent, of which 467 were personal in nature.[43] The 467 messages were sent over a 40 working day timeframe. The central issue in this case was whether or not the content of the messages was exempt from public disclosure because they were personal and would provide no information on government functions. Nevertheless, this case clearly demonstrates the necessity for employers' policies regarding Internet use and the monitoring thereof.

Computer or Internet misuse is not limited to employees who are required to use a computer for the completion of their duties. Carla Tojino was fired from her job at Northwestern University when it was discovered she had downloaded 2,000 MP3 music files on her computer at work.[44] Ms. Tojino claimed she simply enjoyed listening to background music; her primary responsibilities included writing thank-you notes by hand to university contributors.[45] Computer misuse transcends all types and levels of employees and does not appear limited to workers located within the United States. For the first time, an employment tribunal in Liverpool, England, upheld the dismissal of an

---

[41] *Id*. at 1106.
[42] *Id.*
[43] *Id*. at 1107.
[44] *See* Art Golab, *MP3 Music Files Get Worker at Northwestern Fired*, CHICAGO SUN TIMES, Aug. 2, 2000, News at 4.
[45] *Id.*

employee for using the computer at work to make vacation reservations.[46] The vacation was booked but only after the woman had made 150 searches online. "That kind of number is not just somebody tapping in," said attorney Sue Nickerson. "The offence [sic] is theft. The employee is taking money from the employer and using the time to look at the Internet, so depriving the employer of the benefit."[47]

To put the potential loss of employee surfing into perspective, consider the following:

> An employee with a monthly salary of $3,000 costs the company about $20.70 per hour. If he spends 30 minutes accessing the Internet on non-work related websites, the wastage to the company is $10.40 per employee daily—or $217.50 a month. For a company with 200 employees, the wastage will amount to $43,500 a month or $522,000 a year, representing up to 6.26 percent of the company's annual wage cost.[48]

Besides the actual time lost from "cyberloafing,"[49] an often-uncounted cost is the strain to a company's Internet system. Constant improper use results in a system slowdown that affects all employees and customers. The more bandwidth that is consumed by non-work related surfing, the less that is available for work-related projects. For instance, in December of 1998, Navistar International Corporation's e-mail administrator Todd Purifoy devoted considerable time trying to slow the proliferation of a game titled "Elf Bowling." The game, which comes via an e-mail attachment, takes up about 1 Mbyte. Purifoy said if every one of Navistar's 10,000 employees had decided to send copies of the game to friends and relatives, it could have brought down the

---

[46] *See* Ian Herbert, *Court Backs Dismissal of Net Surfer*, LONDON INDEPENDENT, June16,1999, at 10.
[47] *Id.*
[48] Chen Bin, *Preventing Internet Misuse in the Office*, BUS. TIMES SINGAPORE, June 18, 2001, at SS13, Say IT.
[49] "Cyberloafing" occurs when employees use the Internet for personal endeavors. *See* Jon Tevlin, *supra* at 11.

company's e-mail servers "in no time."[50] In addition, when bandwidth is charged by volume, the loss to the employer is even higher.[51]

Cyberloafing also can be costly to employers in lost productivity and lost revenue from defending lawsuits brought by discharged employees. This point is illustrated by *Sherrod v. AIG Healthcare Management Services, Inc*.[52] Sherrod was hired by AIG as a clerk typist in 1989 for $17,000. She was promoted and received salary increases several times. In 1995, she was promoted to Systems Trainer where she traveled to AIG sites to train people on data entry for medical billing.[53]

In 1991, Sherrod had been informed that use of office equipment for personal activities was prohibited.[54] In 1997, the regional director received a report that Sherrod had a picture of a naked man on her computer and that she might be operating a dating service from her office. An internal investigation indicated no proof of a dating service, but the investigator found 23 inappropriate pictures on her computer, including two pictures of erect, naked men and two revealing photographs of the plaintiff.[55] Sherrod was terminated for downloading pornography on the Internet. In response, Sherrod filed a lawsuit claiming her employer violated the Age Discrimination in Employment Act and the Equal Pay Act. The United States District Court granted the employer's motion for summary disposition.[56] Employers today face not only defending unsubstantiated

---

[50] Thomas York, *Invasion of Privacy? E-Mail Monitoring is on the Rise*, INFORMATIONWEEK.COM, Feb. 21, 2000, http://www.informationweek.com/774/email.htm
[51] Chen Bin, *supra* at 48.
[52] Sherrod v. AIG Healthcare Management Services, Inc., 2000 U.S. Dist. LEXIS 1626 (N.D. Texas).
[53] *Id*. at *2.
[54] *Id*. at *3.
[55] *Id.* at *4.
[56] *Id.* at *17.

wrongful termination cases, but also must be diligent to prevent unwelcome behaviors such as this that can create a hostile work environment for other employees and expose the employer to further potential liabilities.

Security issues are also at stake for the employer. A major concern about e-mail and Internet access is that they open avenues through which employees might send out company secrets, inadvertently or not.[57] When intellectual property and sensitive corporate information pass through e-mail on a regular basis, it is essential that employers have clear policies about what may or may not pass via the Net. Policies may not be enough; filtering software may be required.

Monitoring software was recently at issue in the Ninth Circuit Court of Appeals after it was discovered that federal judicial employees had improperly downloaded music from Napster, played Internet games like the fantasy battle game Quake and visited other "inappropriate websites." A federal judiciary committee argued that such usage raised "immediate and continuing security vulnerabilities."[58] Going into sites such as Napster, it was warned, creates "tunnels" hackers could use to dig back into the court's computers. Further, it was alleged that attempts to hack the court's computers had been detected from China and Australia to all over the United States.[59]

Another concern is that some of the attachments and video clips sent through e-mail systems might have viruses in them, which could cause a computer to crash—or possibly

---

[57] *See* Leyla Kokmen, *Firms E-Mull Computer Policies: Employees' Personal Use a Concern*, DENVER POST, Mar. 22, 1999, at E-01.
[58] *See* Michael Hedges, *Big Brother Watching Federal Staffers: New Guidelines Bar Employees from Improper Use of the Internet*, HOUSTON CHRON., Aug. 14, 2001, at A4.
[59] *Id.* The judges were not impressed. Mary Schroeder, Chief Judge of the U.S. District Court for the 9th Circuit in Northern California, ordered the intrusion detection software disabled for that federal circuit, citing privacy issues and lack of advanced notice. *Id.*

an entire floor's worth of computers.[60] According to the International Computer Security Association (ICSA), three out of four organizations experienced a virus in 1998, up from 68% in 1997.[61] A 1998 Computer Security Institute (CSI) survey cited financial losses of $136 million due to computer invasions—an increase of 36% since 1997.[62]

Finally, legal liability issues, in addition to sexual harassment or hostile work environments, seem to justify monitoring systems. Such issues include online defamation (otherwise referred to as "cyberlibel"), violations of securities laws (utilizing the computer to engage in insider trading), violations of the NLRB for disallowing union correspondence, and software piracy. Websense, Inc., reports that the number of pirated software and hacking web sites has increased more than 240 percent in the last year alone, now totaling 5,400 sites representing 800,000 web pages.[63] There are several problems with pirated software, all of which cost the company time and money. First, employees with pirated software drain helpdesk resources by trying to support programs unauthorized by the company. Second, employees expose their employers to legal liability by copying illegal software. Finally, downloading large software packages create an additional burden on the network, sapping bandwidth that could be used for work-related applications.[64]

In truth, employers face tremendous legal liability over a medium that appears to be fleeting in nature to the user but permanent in effect. One of the biggest problems with electronic mail is that old e-mails can be drudged up and used in lawsuits against

---

[60] *See* Kokmen, *supra* at 57.
[61] *See Increased Popularity of Pirated Software Creates Legal Liability and Bandwidth Headaches for Corporations*, WEBSENSE, Oct. 30, 2001, http://www.websense.com/company/news/pr/01/013001.cfm.
[62] *Id.*
[63] *Id.*

companies, as they were in the antitrust suit against software maker Microsoft Corporation.

In *Schwenn v. Anheuser-Busch, Inc.*,[65] the U.S. District Court for the Northern District of New York allowed Schwenn to submit copies of the e-mails she received at work to prove her sexual harassment case against Anheuser-Busch. Schwenn was permitted to use the e-mail messages even though they had already been deleted from Anheuser-Busch's e-mail system. Schwenn was ultimately unsuccessful in her claim because her allegations were considered minor in the realm of a "hostile work environment." However, this decision does create a precedent that is potentially dangerous to employers by holding that deleted e-mail messages can form a basis for employer liability.

Also problematic are chain e-mails that contain jokes or cartoons, inflammatory or volatile opinions, threats or racist remarks. Current sexual harassment and discrimination law is not prepared to deal with certain issues that arise out of the use of the Internet and e-mail. Only a few states have enacted laws that make any harassment through the use of the computer a crime.[66] Plaintiffs are able to use e-mails affirmatively against their employers because stored computerized messages last seemingly forever. In fact, plaintiffs' attorneys are now demanding computerized information as a regular part of their discovery requests, creating an additional expense to employers.[67] Evidence in the form of sexually oriented or harassing computer messages can bolster an employee's claim. Even e-mail and Internet messages that presumably have been deleted often can

---

[64] *Id.*
[65] 1998 U.S. Dist. LEXIS 5027 (N.D.N.Y. 1998).
[66] *See e.g.*, CALIF. PENAL CODE § 646.9(g) (West 1998); CONN. GEN. STAT. ANN., §§ 53a-182b, 53a-183 (West 1995).
[67] *See* Christine A. Amalfe and Kerrie R. Heslin, *Courts Start to Rule on Online Harassment*, NAT'L L.J., Jan. 24, 2000, at C1.

be retrieved. Employers could be required to furnish existing hard copies of computerized messages, produce information on computer disks or provide new printouts. The time and expense of reviewing these communications, as well as copying and printing these documents, pose a new burden for defense litigation. Note, however, there is one bright light: While e-mails can provide evidence for the plaintiff, they also can help the defendant if the company can find that the employee harassed everyone, not just members of protected groups.[68]

IV. ONLINE SEXUAL HARASSMENT AND HOSTILE WORK ENVIRONMENT

An increasing number of employees receive access to the Internet through their work computers which heightens the potential for sexual harassment claims by co-employees exposed to inappropriate and offensive screen savers, software, e-mails, and pornographic web sites while at work. When responding to allegations of sexual harassment it is imperative that employers respond promptly and appropriately to successfully defend such claims.

In *Stuart v. General Motors Corporation*,[69] Lora Stuart was employed for eleven years as a Journeyman electrician. In July 1996, she informed her supervisor that a computer in her work area had a pornographic program, that she was subjected to unwelcome sexual remarks, and that her work environment was hostile.[70] GMC managers promptly removed the computer, began an investigation, and offered Stuart the same position elsewhere in the plant, which she declined. Subsequently, Stuart found pornographic photographs posted by other employees in and on her locker. Between July 1996 and

---

[68] *See* Jon Tevlin, *supra* at 11.
[69] 217 F.3d 621 (8th Cir. 2000).
[70] *Id*. at 626.

January 1997, Stuart was disciplined numerous times for taking excessive breaks, insubordination, and tardiness.[71] In January 1997, Stuart was terminated for allegedly engaging in a sex act with a male co-worker in an advisor's office.[72] Stuart denied the allegation and claimed she was terminated as retaliation for her sexual harassment claim. The U.S. District Court denied Stuart's claims of a sexually hostile work environment and retaliation. The Court of Appeals affirmed the decision, stating that Stuart failed to complain about the incidents prior to 1996 when she was disciplined for long breaks and did not take action when the sexual harassment incidents actually occurred.[73] Additionally, she refused the transfer when it was offered. Further, GMC was prompt in taking remedial action and investigating her sexual harassment claim.[74]

It is clear that employers in this millennium are confronted with entirely new complications and challenges when combating sexual harassment at work, especially given the advanced technology available to most employees. The Internet has dramatically impacted the speed and access to communication by employees which has heightened the risk encountered by employers for sexual harassment claims. For example in *Strauss v. Microsoft Corporation,*[75] the federal district court of New York determined that Strauss had successfully brought a prima facie case against her supervisor for discrimination based on the supervisor's refusal to promote her. The employer responded to the claim by arguing that Strauss was not discriminated against but was not given the promotion because she was not qualified for the position. However, the federal district court denied the employer's motion for summary judgment,

[71] *Id*. at 628.
[72] *Id.* at 629.
[73] *Id.* at 632.
[74] *See id*. at 633.

indicating that the jury could find gender discrimination based on Strauss's evidence of sexual and offensive e-mails sent to her by her supervisor.[76]

In a related case, *Knox v. State of Indiana*,[77] the U.S. Court of Appeals affirmed a jury's verdict in Knox's favor based on a claim of sexual harassment and retaliation. Kristi Knox was employed as a correctional officer in a correctional facility in Indiana. Knox's immediate supervisor sent her e-mail messages requesting sex and asking if she wanted to have a good time. He also repeatedly left phone messages, asked her out on dates, and reminded her to check her e-mail. The supervisor initially denied Knox's complaint until the investigator indicated that he had copies of the e-mail.

In *Burlington Industries, Inc. v. Ellerth*,[78] and *Faragher v City of Boca Raton*,[79] the United States Supreme Court set forth the standards for establishing sexual harassment under which an employer would be liable and the applicable affirmative defenses. Although these particular cases did not involve the Internet or computer usage,[80] the law changed dramatically when the Court issued these twin opinions. Specifically, the Court held that the "dissemination of sexually oriented material may form the basis of a hostile work environment claim. Hostile work environment sexual harassment exists when an

---

[75] 814 F. Supp. 1186 (S.D.N.Y. 1993).
[76] *Id*. at 1194.
[77] 93 F.3d 1327 (7th Cir. 1996).
[78] 524 U.S. 742 (1998).
[79] 524 U.S. 775 (1998)
[80] In Burlington, Kimberly Ellerth was employed as a salesclerk for 15 months at Burlington Industries. She alleged that she was confronted with frequent sexual advances by the vice president (the boss of her immediate supervisor). Ellerth knew about Burlington's sexual harassment policy but failed to file a complaint with the company. Ellerth did not respond to the advances and was still promoted. In Faragher, Beth Ann Faragher was employed as a part-time lifeguard for the City of Boca Raton in Florida. She argued that male supervisors made lewd and offensive remarks and inappropriately touched her. The City of Boca Raton did have an anti-harassment policy but it had not

employee is subject to unwelcome sexually harassing conduct that creates an intimidating, offensive or hostile working environment."[81] Further, the court held that "an employer is subject to vicarious liability to a victimized employee for an actionable hostile environment created by a supervisor with immediate (or successively higher) authority over the employee."[82] Any type of exposure to inappropriate pictures, language or conduct could theoretically make the employer liable, whether the offensive material be oral or in writing, or from traditional sources or non-traditional sources such as the Internet or e-mail messages.

Even after the strong message sent in *Ellerth* and *Faragher*, the number of sexual harassment cases involving use of the Internet continues to increase. In *Coniglio v. City of Berwyn*,[83] the U.S. District Court of Illinois determined that Coniglio could proceed on her claim that the City of Berwyn had placed her in a hostile work environment when her supervisor, the comptroller, used his office computer to retrieve pornographic pictures which he openly displayed on his computer 12.5 feet away from Coniglio's desk. The supervisor regularly called his employees into his office, including Coniglio, where the pornographic images were displayed on his computer screen in order to prompt a reaction from his employees regarding the pornography. After Coniglio made her official complaint, she mysteriously began receiving unsolicited e-mails from various pornographic websites. On dismissing the defendant's motion for summary judgment,[84]

---

been distributed to the lifeguards. Faragher also did not inform the city managers of her harassment.

[81] Christina A. Amalfe and Kerrie R. Heslin, *supra* at 67

[82] Jane Howard-Martin and Christopher K. Ramsey, *Supreme Court Stresses Employer Action to Prevent and Correct Sexual Harassment by Supervisors*, METROPOLITAN CORP. COUNSEL, Mid-Atlantic Ed., at 7.

[83] 1999 U.S. Dist. LEXIS 19426 (N.D. IL. 1999)

[84] Coniglio v. City of Berwyn, 2000 U.S. Dist. LEXIS 9841 (N.D. IL 2000).

the court was "unconvinced" a hostile environment had not been created just because the plaintiff had to look through a window from another office to see the computer. In any event, plaintiff and other witnesses testified they could see the pictures while passing the defendant's office. "Defendants can hardly expect the courts to seriously consider a defense to a sexual harassment claim that would create an obligation for employees to actively ignore offensive behavior occurring in front of them."[85]

In a similar case, *Scott v. Plaques Unlimited, Inc.*,[86] Scott was an eighteen-year old female employed as a telemarketer for Plaques Unlimited. Her immediate supervisor made personal comments about her appearance and her personal relationships. Scott also found her supervisor and a customer viewing pornography on the Internet and found Playboy magazines in his office. Scott resigned her position after returning from the employer's trade show where her supervisor rubbed her legs and feet under the table. Additionally, she was told that she should bend over to pick things up, stick out her chest, and to giggle at what male customers said in order to enhance sales.

One recent case that will undoubtedly have a tremendous impact on employer liability for what is posted on company-approved Internet sites is *Blakey v. Continental Airlines, Inc.*[87] In 1989, Tammy Blakey became the first female captain to fly an airbus for Continental.[88] Blakey was hired by the airlines in 1984.[89] Soon after Blakey qualified as a captain for Continental, she complained to the airline that her male co-workers were sexually harassing her and creating a hostile work environment.[90] In 1991, Blakey

---

[85] *Id.* at *22.
[86] 46 F. Supp.2d 1287 (M.D. Fla. 1999).
[87] 751 A.2d 538 (N.J. 2000).
[88] Blakey v. Continental Airlines, Inc., 992 F. Supp. 731, 733 (D. N.J. 1998).
[89] *Id.*
[90] Blakey, 751 A.2d at 539.

regularly filed complaints with the appropriate representatives of Continental regarding pornographic pictures and inappropriate, vulgar comments, which were directed to her while in the workplace.[91]

In 1993, Blakey filed a claim for sexual discrimination and retaliation in violation of Title VII of the Civil Rights Act of 1964 and 1991 against Continental in federal court and with the Equal Opportunity Commission.[92] During this time, other pilots posted gender-based and harassing messages on the pilot's on-line computer bulletin board called "The Crew Members Forum." Following an unsuccessful attempt to amend her federal complaint, Blakey filed suit in the Superior Court of New Jersey seeking damages for defamation against Continental Airlines and certain co-employees individually.[93] That court dismissed Blakey's claims against the individual defendants on the basis of lack of personal jurisdiction. The court also declined to impose vicarious liability on Continental for remarks uttered by its employees regarding her.[94] On appeal, the New Jersey Superior Court Appellate Division held that Continental was not responsible for the harassment because the pilots' messages were not performed as part of the pilot's job duties.[95] Conversely, the Supreme Court of New Jersey held that "[i]f the employer had notice that co-employees were engaged on such a work-related forum in a pattern of retaliatory harassment directed at a co-employee, the employer would have a duty to

---

[91] *Id.*

[92] Initially, Blakey filed a complaint against Continental in the U.S. District Court in Seattle, Washington. Upon Continental's motion, the actions were transferred to the U.S. District Court of New Jersey. *See* Blakey v. Continental Airlines, Inc. 992 F.Supp. 731 (D.N.J. 1998). After a five week trial, the jury found Continental liable for sexual harassment and awarded Blakey $875,000. This award was later lowered to $625,000. *Id*. at 742.

[93] Blakey, 730 A.2d 854 (N.J. Super. 1999).

[94] *Id.* at 856.

[95] *Id*. at 868.

remedy that harassment."[96] The court reasoned that conduct by employees outside the workplace might, in fact, infiltrate the work environment.[97]

The Blakey decision clearly demonstrates that we have entered a new frontier with cyberspace issues that employers must consider when making policies and when monitoring employees to ensure a non-hostile work environment.

Employers are not completely defenseless against such claims; however, employers should take proactive action by: establishing preventive programs, promptly and properly investigating complaints, and establishing specific deterrent policies.[98] These guidelines should include sexual harassment and discrimination policies and the prohibition of such acts by employees in person, by written communication, and in the form of electronic communication. "As the U.S. Supreme Court articulated in *Faragher*[99] and *Ellerth*,[100] if an employer exercises reasonable care to prevent and correct sexually harassing behavior and the employee fails to take advantage of these preventive and corrective opportunities, the employer can sometimes raise an affirmative defense to liability."[101] In some cases, particularly earlier cases, employers were successful at obtaining summary disposition because the Court recognized the employer's use of reasonable care by disciplining employees and by implementing appropriate policies as was evidenced in *Stuart v. General Motors Corporation.*[102]

---

[96] *See* Blakely, 751 A.2d at 543.
[97] *Id*. at 549.
[98] *See* Christine A. Amalfe and Kerrie R. Heslin, *supra* at *67; Cases Weigh Employer Liability for Employees' Use of E-Mail, Chat Rooms and Porn Sites*, N.J.L.J., June 12, 2000.
[99] Faragher, 524 U.S. at 775.
[100] Burlington, 524 U.S. at 742.
[101] *See* Faragher, 524 U.S. at 775.
[102] 217 F.3d 621 (8th Cir. 2000).

However a recent case, *Harrison v. Eddy Potash Inc*.,[103] raises the bar of *Faragher* and *Ellerth* for the circumstances under which an employer can avoid liability for the sexual harassment conduct of its supervisors. In this case, Jeanne Harrison was the only woman working as an underground potash miner with 30 men. Harrison's direct supervisor was responsible for delegating duties and work assignments to her. He was also involved in vacation schedules and the company's disciplinary process. From May through June of 1993, Harrison's supervisor tried to kiss her, touched her, forced her to fondle him, and made sexually suggestive comments to her. Two months after the sexual harassment started, Harrison complained to a safety officer. The company immediately began an investigation and placed Harrison on administrative leave that day. Seven days later the human resource manager issued a report and paid back wages, counseling, and medical expenses to Harrison. The company also transferred Harrison to another crew. Her supervisor was reprimanded, placed on probation, and told to have no contact with Harrison.

Harrison filed suit and Eddy Potash, Inc., argued that it exercised reasonable care in handling the complaint and that it had a sexual harassment policy in place at the time of the incident. Eddy Potash unsuccessfully attempted to utilize the affirmative defenses of *Faragher* and *Ellerth* by demonstrating the company had taken prompt remedial action and should not be held vicariously liable.

The United States Court of Appeals for the Tenth Circuit has made clear in this case that employers are expected to do more than just develop a sexual harassment policy and promptly respond when a complaint is filed. The court stated that employers must make certain that supervisory employees are looking out for all types of potentially harassing

[103] 248 F.3d 1014 (10th Cir. 2001).

behavior and that all employees are aware of the company's harassment policy by receiving a copy of the policy, that employees receive appropriate training, and that the policy is regularly enforced. In the *Harrison* case, the plaintiff was never informed of the policy, and non-supervisory employees were not given copies of the sexual harassment policy. In fact, the policy was not posted on the mine bulletin boards nor was it posted in the changing room of the female miners. The court felt that Eddy Potash largely ignored the company's sexual harassment policy. Thus, the court believed that the jury could conclude that Eddy Potash, Inc., had exercised something less than "reasonable care" in preventing Harrison from being subjected to the sexual harassment engaged in by her supervisor. Therefore, the Tenth Circuit found Eddy Potash liable for the acts of sexual harassment committed by Harrison's supervisor. This ruling could impose some additional requirements on employers for their Internet policies and computer usage as well.

V. CONSTITUTIONAL ISSUE – FOURTH AMENDMENT

The Fourth Amendment provides a general right of privacy in the United States Constitution.[104] It is well settled, however, that the Fourth Amendment protects people from unreasonable searches and seizures performed by the government, and does not necessarily apply to searches performed by private parties.[105] Therefore, unless the

[104] The Fourth Amendment to the Constitution provides that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . ." U.S. CONST. AMEND. IV. While the amendment does not explicitly protect or name a right to privacy, the U.S. Supreme Court has found it to fall within the ambit of the amendment. *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965).

[105] *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 113-14 (1984) (stating that a search or seizure performed by a private individual, "even an unreasonable one," is not proscribed by the Fourth Amendment).

government employs a person, the Fourth Amendment does not offer a protection of privacy in that employee's e-mail. In order for the protections of the Fourth Amendment to cloak an individual against intrusive governmental searches and seizures, a judicially construed threshold must first be crossed. The United States Supreme Court in *Katz v. United States* ruled that the constitutional protections embodied in the Fourth Amendment are only triggered upon the showing of a reasonable expectation of privacy.[106]

In *Leventhal v. Knapek,*[107] Gary Leventhal was a grade 27 employee with the New York Department of Transportation (DOT) in the Accounting Bureau.[108] He also maintained his own tax practice on the side, which was approved by DOT.[109] The DOT had a written policy prohibiting theft, which included use of DOT equipment for personal use.[110] The DOT also had a written policy prohibiting the loading of unlicensed software on DOT computers. Yet, Leventhal's direct supervisor informed employees that it was all right to use unlicensed software due to budget constraints.[111] In October of 1996 an anonymous letter was mailed to the New York State Office of the Inspector General alleging that a grade 27 employee spent a great deal of time on non-work related business, was regularly late for work, and was frequently absent.[112] The letter also stated

[106] 389 U.S. 347, 361 (1967) (Harlan, J., concurring)
[107] 266 F.3d 64 (2nd Cir. 2001).
[108] *Id.* at 67.
[109] *Id.*
[110] *Id.*
[111] *Id.*
[112] *Id.* at 68.

that many other employees were incompetent as well and played computer games for a long time each day.[113] This letter prompted an investigation.

Leventhal was the target of the investigation since he was the only grade 27 employee in the Accounting Bureau. The investigators searched and copied files from Leventhal's computer without his knowledge or consent.[114] They found unauthorized tax preparation software and tax file names.[115] Leventhal admitted printing tax returns from his office computer. After Leventhal settled his DOT charge he brought suit against those involved in the DOT investigation claiming that the search of his computer was in violation of his Fourth Amendment rights.[116]

The Second Circuit determined that "[a] public employer's search of an area in which an employee had a reasonable expectation of privacy is 'reasonable' when 'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of' its purpose."[117] The court found that although Leventhal had some expectation of privacy in his office, his Fourth Amendment rights were not violated by the actions of the DOT. Quoting *O'Conner v. Ortega,*[118] the court stated that "[a]n investigatory search for evidence of suspected work-related employee misfeasance will be constitutionally 'reasonable' if it is 'justified at its inception' and of appropriate scope."[119] Thus, the Leventhal case shows that public employees may have an

---

[113] *Id.* "…A grade 18 with an apparent alcohol problem …is so incompetent that his supervisor allows him to sleep at his desk…."
[114] *Id.*
[115] *Id.* at 69. Investigators found "PPU," a program likely to contain tax software because of the file names "TAX.FNT" and CUSTTAX.DBF." *Id.*
[116] *Id.* at 71.
[117] *Id.* at 73 (citing O'Conner v. Ortega, 480 U.S. 709, 726 (1987)(plurality opinion)).
[118] 480 U.S. 709 (1987).
[119] Leventhal, 266 F.3d. at 75 (citing O'Conner, 480 U.S. at 726).

expectation of privacy in the workplace but that the employer has a very low threshold for justifying such a search.

In *United States v. Simons*,[120] the Fourth Circuit Court of Appeals held that a government worker did not have a legitimate expectation of privacy with regard to the records of his Internet use in light of his government employer's policy. Mark Simons was employed as an electronic engineer at the Foreign Bureau of Information Services (FBIS), a branch of the Central Intelligence Agency.[121] FBIS provided him with an office he did not share with anyone and an office computer with Internet access. FBIS also provided him with a copy of its policy regarding Internet usage. The policy specifically stated that employees were to use the Internet for official government business only, prohibited accessing specific illegal materials and warned that FBIS would conduct electronic audits to ensure compliance.[122] The policy highlighted specific information the electronic audits would be capable of recording[123] and stated that "users shall . . . understand FBIS will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate."[124]

Upon entering the word "sex" into the firewall of the computer system, the manager discovered a large number of "hits" originating from Simons' computer.[125] Investigators determined that the websites contained pictures of naked women. Further investigation

---

[120] 206 F.3d 392 (4th Cir. 2000), *cert. denied*, 534 U.S. 930 (2001).
[121] *Id*. at 395.
[122] *Id.* at 395-96.
[123] *Id*. at 396. Specifically the policy advised all employees that the electronic audit mechanisms would be capable of recording: "access to the system, inbound and outbound file transfers; terminal connections…sent and received e-mail messages; Web sites visited, including uniform resource locator (URL) of pages retrieved; and the date, time, and user associated with such event." *Id*.
[124] *Id.*
[125] *Id*.

revealed that Simons had downloaded over 1000 pictures that were pornographic in nature.[126] From a separate workstation, investigators were able to copy and examine all of the files on Simon's computer without entering his office. It was determined that some of the pornographic pictures were those of minors. Criminal investigators physically entered Simon's office once to remove and replace his hard drive.[127] Search warrants were subsequently issued and carried out.[128]

Simons argued that the warrantless searches of his computer files and office violated his Fourth Amendment rights. The Court held that the remote searches of Simons' computer did not violate his Fourth Amendment rights because, "in light of the Internet policy, Simons lacked an expectation of privacy in the files downloaded from the Internet."[129] Although Simons possessed an expectation of privacy in his office, since it was his office alone, one exception to the warrant requirement is the government's interest in the "efficient and proper operation of the workplace."[130] Citing *O'Connor v. Ortega*,[131] the court held that when a government employer conducts a search pursuant to an investigation of work-related misconduct, the Fourth Amendment's protections are satisfied so long as the search is reasonable in its inception and scope.[132]

VI. FEDERAL AND STATE STATUTES

---

[126] *Id.*
[127] *Id.*
[128] *Id.* at 397. "The warrant mentioned neither permission for, nor prohibition of, secret execution." *Id*. Yet the search was conducted during the evening when Simons was not there. The search team *copied* computer files found on his zip drive and diskettes, the entire contents of his computer, computer diskettes found in various locations within his office, videotapes, and various documents, including personnel communication. *Id*.
[129] *Id*. at 398.
[130] *Id.*at 400 (citing O'Connor v. Ortega, 480 U.S. 709, 723 (1987)(plurality opinion))
[131] 480 U.S. 709, 725-26.
[132] *Id*. at 400.

Federal statutes appear to offer some protection for the privacy of e-mail in the workplace. A statutory framework concerning electronic communications exists in the Electronic Communications Privacy Act of 1986 (ECPA).[133] The ECPA is an amendment to Title III of the Omnibus Crime Control and Safe Street Act of 1968,[134] and was passed in recognition of the need to update privacy protection in order to remain abreast of quickly changing and developing technology. The amendment expanded the scope of Title III to include the interception of "electronic communication" and unauthorized access of stored electronic communications.[135] The disclosure and dissemination of information obtained in violation of the statute are also prohibited.[136] Additionally, while the transmission of communications is protected from interception by section 2511 of the Act, a provision was also included to protect the electronic storage of the communications.[137]

Although the legislative history of the ECPA indicates that e-mail was intended to fall within the ambit of the Act's protection,[138] provisions and exceptions limit that protection and, in reality, permit employers in a private company to access the e-mail of their employees without violating the statute. Generally, the statutory language creates an "ordinary course of business" exception, an exception under the stored communications

[133] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126 (2001).
[134] 18 U.S.C. §§ 2510-2520 (2001).
[135] *See* 18 U.S.C. §§ 2510(1), (4), (12), (17) (2001).
[136] 18 U.S.C. § 2511(c) – (d) (2001).
[137] *See* 18 U.S.C. § 2701 (2001).
[138] S.Rep.No.541, 99th CONG., 2D SESS., at 14 1986). *See also* Thomas R. Greenberg, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 236 (1994).

provisions, a limitation under the commerce clause, and an exception based on consent.[139]

The relevant portions of the ECPA are as follows:

> As used in this chapter
> (1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origins and the point of reception…
> (4) "intercept: means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device.
> (5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than:
> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business…
> (12) "electronic communication" means any transfer of signs, signals, writing images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
> (A) any wire or oral communication;
> (13) "user" means any person or entity who—
> (A) uses an electronic communication service; and
> (B) is duly authorized by the provider of such service to engage in such use…[140]

First, the ECPA retains language which establishes an "ordinary course of business" exception. The definition of "device" specifically excludes any telephone or component "furnished to the subscriber or user by a provider of [the]. . . communication service in the ordinary course of its business and being used by the subscriber in the ordinary course

[139] *See* 18 U.S.C. §§ 2510(5)(a)(i), 2701(c)(a), 2501(12), 2511(2)(d) (2001).
[140] 18 U.S.C. §§ 2510 (2001).

of its business . . .."[141] If components are not with this definition of device, interception of e-mail would be permitted by this provision.

Second, there is some confusion in the definition of the company as a "provider" or an agent to the provider. If the employer is read to be an owner of a private network or an agent to the provider, the door is opened to monitoring by the employer under the stored communications provision. According to the provision, it is lawful to access stored communications if it is done pursuant to authorization "by the person or entity providing a wire or electronic communications service."[142] Therefore, if a company that supplies e-mail service to its employees is seen as a service provider, only a simple authorization from the company is required to access the stored messages received and sent by its employees.

Third, the definition of "electronic communications" under the ECPA is limited to communications and systems which "affect interstate or foreign commerce."[143] It is conceivable that a small intra-company system, which does not cross-state lines, may not be covered by the ECPA. However, in accessing the Internet itself, usually state lines are crossed.

---

[141] *See* 18 U.S.C. § 2510(5)(a)(i) (2001).

[142] 18 U.S.C. § 2701 (a)(1-2); 18 U.S.C. § 2701(c)(1) (2001) provides:

"(a)(1) [w]hoever intentionally accesses without authorization a facility through which an electronic communication service is provided or (2)…obtains [or] alters…electronic communication while it is in electronic storage in such system shall be punished…"

(c) Exceptions. Subsection (a) does not apply with respect to conduct authorized…

(1) by the person or entity providing a wire or electronic communications service…"

Id.

[143] *See* 18 U.S.C. §§ 2510(1), 2510(12) (2001).

Finally, under the ECPA, interception of communications is permitted where one of the parties to a communication has given prior consent.[144] Implied consent may exist if the company has a policy on e-mail or Internet usage and the employee has been made aware of such policies.

Other legislation aimed at providing greater protection to employees' use of e-mail has been proposed by Congress but not yet been adopted. The Privacy for Consumers and Workers Act was proposed in 1993,[145] but did not materialize. It would have required employers to inform their employees of workplace monitoring and establish limits on the scope of the monitoring.[146]

Some states also have statutes that limit the interception of electronic communications. Although states are free to enact measures which restrict employer monitoring further than the federal statute, many of the states which have statutes simply incorporate the ECPA exceptions pertaining to consent and business use.[147] Thus far, only California has had a bill pass prohibiting employers from monitoring employees' e-mail or computer files unless the employee had signed an agreement acknowledging the employer's right to monitor.[148] However, Governor Gray Davis vetoed the legislation last September 2000.[149]

---

[144] 18 U.S.C. § 2511(2)(d) (2001)("It shall not be unlawful under this chapter…where one of the parties to the communication has given prior consent to such interception…") *Id.*

[145] *See* H.R. 1900, 103d Cong., 1st Sess. (1993).

[146] *Id.*

[147] *See* Laurie Thomas Lee, *Watch Your E-Mail, Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop*, 28 J. MARSHALL L. Rev. 139, 175 (1994) (outlining state statutes with prior consent and business use wiretap exemptions – Table 2).

[148] *See* Cal. Senate Bill 1822 (2000).

[149] Allison R. Michael and Scott M. Lidman, *Privacy: Technology Advances Bring Increased Monitoring*, EMPL. L. STRATEGIST, March 2001.

VII. COMMON LAW – INVASION OF PRIVACY TORT

One area where an employee might find protection is under a common law suit for invasion of privacy.[150] Under the tort of invasion of privacy, "intrusion into seclusion or private affairs" applies most aptly in the context of e-mail in the workplace. This tort is committed by "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, . . . if the intrusion would be highly offensive to a reasonable person."[151]

In *McLaren v. Microsoft Corp.*,[152] Microsoft Corporation employed Bill McLaren. He was suspended in December 1996 pending the outcome of an investigation pertaining to sexual harassment and "inventory questions." McLaren requested that Microsoft allow him access to his e-mail so he could disprove the claims against him. Microsoft told McLaren he could only access his e-mail information through a company official. McLaren was terminated from Microsoft on December 11, 1996. McLaren then filed suit alleging invasion of privacy. He argued that Microsoft had effectively "broke into" his personal e-mail files and that he had "a legitimate expectation of privacy in the contents of the file," because Microsoft allowed him to have a personal password for his folders. McLaren believed that his folders would be free from "intrusion and interference."

---

[150] Invasion of privacy is composed of four separate torts: 1) unreasonable intrusion upon the seclusion of another, 2) appropriation of another's name or likeness, 3) unreasonable publicity given to the other's private life, and 4) publicity that unreasonably places the other in a false light before the public. RESTATEMENT (SECOND) OF TORTS § 652A(2) (1977).

[151] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[152] 1999 LEXIS 4103 (Tex. App. 1999).

As support for his contention that he had an expectation of privacy, McLaren cited *K-Mart Corp. Store No. 7441 v. Trotti.*[153] In *Trotti*, the manager at K-Mart searched the lockers and the purse of Billie Trotti, a store clerk. He was searching for a stolen watch, but did not believe Trotti had taken it. Trotti provided her own lock for her locker. The court reasoned "that the locker was the employer's property and, when locked, was subject to legitimate, reasonable searches by the employer."[154] The court recognized that if the employer provided the lock or combination, it in fact was retaining control over the locker. However, the court concluded that when the employee uses his or her own lock then the "employee manifested, and the employer recognized, an expectation that the locker and its contents would be free from intrusion."[155]

McLaren unsuccessfully argued that the Trotti locker was analogous to his e-mail folders. The court disagreed, stating that McLaren's workstation and computer were given to him so he could "perform the functions of his job" whereas the locker in the Trotti case was for the storage of Trotti's own personal items.[156] Also, because McLaren was under investigation at the time Microsoft intercepted his e-mail, the interception was not viewed as "highly invasive." Thus, the court concluded that Microsoft'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."

---

[153] 677 S.W.2d 632 (Tex. App. 1984), *writ ref'd n.v.e.*, 686 S.W.2d 593 (1985).
[154] *Id.* at 637.
[155] *Id.*
[156] McLaren, 1999 LEXIS 4103, at *11.

In *Smyth v. Pillsbury*,[157] Michael Smyth brought a wrongful discharge claim against the Pillsbury Company for wrongfully terminating him from his position as regional operations manager. Pillsbury had an e-mail system for internal communications. Employees were told that all e-mails would remain privileged and confidential and that e-mail messages would not be intercepted or used against employees as a reason for termination or reprimand.

Smyth sent an e-mail message that was intercepted by his employer. The message said, "Kill the backstabbing bastards" which was in reference to management. Smyth also referred to the holiday party as a "Jim Jones Koolaid Affair."[158] Smyth was terminated for sending unprofessional and inappropriate messages.

Smyth argued that his termination from Pillsbury was wrongful since it was in violation of public policy precluding employers from violating an employee's right to privacy.[159] The court held that Smyth did not have a reasonable expectation to privacy for e-mail messages sent over Pillsbury's e-mail system, regardless of the company's promise to keep e-mail messages private. The court stated that once the e-mail messages were voluntarily communicated over the company's e-mail system, all expectations of privacy were lost.[160] The court also said that Pillsbury's "interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employees may have in those comments."[161]

These cases demonstrate the unfortunate widening of the gap between employees' right to privacy of e-mail messages and employers' concern with and right to monitor

[157] 914 F.Supp. 97 (E.D.Pa. 1996).
[158] Smyth, 914 F.Supp. at 98, n. 1.
[159] *See id*. at 100.
[160] *Id.* at 101.

employees. As the gap widens, however, the employer may not achieve the benefit it seeks. Rather than preventing and reducing its liability, by implementing monitoring practices, by asserting more detailed control over employee use of the e-mail, and by failing to abide by its own policies, the employer is making itself susceptible to greater liability for the evils committed using e-mail.

Another issue that may arise is monitoring in the context of telecommuting. As more companies utilize telecommuting options (allowing employees to log on to the company network from home), this may be a gray area in the realm of privacy. Once an employee logs onto his employer's network, his employer may have access to his "private files" stored on his home computer. The employer should not have a legitimate business need to examine these files; nevertheless, the employee may be vulnerable to employer snooping.

Some employment relationships may include an employer providing the employee with a home computer. Although this is not technically "telecommuting," the employer will provide the employee with a home computer on which the employee gains access to the company system, and the employee typically writes correspondence for the employer as well as conducts personal business. This is typical with institutions of higher learning, such as colleges and universities.

Indeed, this was the practice at Harvard Divinity School when, in 1998, the dean was asked to resign because of his computer use in the privacy of his official residence.[162] The school owned the dean's home computer, and when he required more memory, the school's technician came to his residence to bring him a new computer and transfer his

---

[161] *Id.*

files. During the course of the transfer, the technician noticed large amounts of pornographic material that had been downloaded from the Internet.

The technician reported the pornographic downloads to his supervisor, and the dean was asked to resign. Although the dean browsed the Internet and downloaded these pictures in the privacy of his own home, and on his own time, the president of the university nevertheless decided that the dean was now unfit to keep his employment. Although an argument could be made that the downloading of pornographic materials is not in keeping with the morals expected of those employed by a Divinity School, it serves to illustrate how precarious a position an employee may find himself in if his employer learns about his private, legal computer activities in the home.

VIII. CURRENT MONITORING PROGRAMS

It is crucial to have effective and fair monitoring policies. But in some cases, a policy by itself may not be enough. To control employee misuse or personal use of telecommunications equipment, twenty-nine percent of the employers surveyed by the AMA said they block Internet connections to unauthorized or inappropriate web sites.[163] Essentially, employee-monitoring software is installed on a company's server. Some packages have a reporting tool that tells the employer how much time is being wasted on accessing certain types of web sites, such as pornographic sites, entertainment, sports, and online trading. All of them allow the employer to block access to certain web sites

---

[162] JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 159 (2000).
[163] AMA Survey, *supra* at 32.

based on detailed categorizations.[164] The following is a brief description of a few of the software monitoring programs available to employers.

OnSecure Computer Software, made by Secure Computing Corporation, identifies improper uses of the Internet by identifying 27 categories of use, including such things as hate speech and pornography, but also such "benign" web sites as entertainment, sports, and investment services. Because of the relative ease with which employees evade filters, this service includes a weekly updating service for that reason.[165]

In 1999, SpectorSoft Corporation released a monitoring program that takes surreptitious "screen shots" of employees' computers at selected intervals for employers to review at a different date.[166] Content Technologies, a United Kingdom-based company, recently launched a software called "Pornsweeper" that examines images attached to e-mails and searches picture files for anything that appears to be flesh.[167] Other Internet filtering programs include MimeSweeper, Mail Essentials, and Message Inspector.

MimeSweeper[168] can filter e-mail with user-defined words or phrases so the Human Resource Department can review the e-mail before it gets to its destination. If an incoming e-mail contains any of those words or phrases, the system grabs and holds it. At that point, human resource staff can review the message. If there is nothing offensive about it, the message can be released. MimeSweeper can be used to block employee access to certain web sites and is used to control the size of incoming and outgoing

---

[164] *Companies are Turning to HR for Control of Workplace Internet Abuse*, HUMAN RESOURCE DEPT. MANAGEMENT REPORT, Jan. 2000.
[165] Jon Tevlin, *supra* at 11.
[166] Allison R. Michael and Scott M. Lidman, *Privacy: Technology Advances Bring Increased Monitoring*, March 2001, EMPL. L. STRATEGIST, at 1.
[167] *Id.*

e-mail. Mail Essentials adds many e-mail security features such as content monitoring, virus scanning and anti-spam filtering. This program only monitors incoming e-mail, not internal e-mail. Finally, Message Inspector goes beyond simple keyword recognition. It detects words according to their meaning in a specific context. The program actually uses the Oxford Dictionary for its analysis of contextual definitions of offensive language.[169]

Companies may have to implement several tools or programs to get the best coverage, depending on their needs: one focusing on monitoring, one focusing on blocking and one that can capture all traffic.

IX. CONCLUSION

The cases in this paper clearly demonstrate that employers should have a policy regarding personal use of the Internet, use of e-mail, and prohibited actions such as surfing and downloading pornographic material and sending sexually harassing e-mail via the Internet or Intranet. However, a blanket policy of "no personal use" may in fact create additional employment law liabilities, particularly involving the National Labor Relations Board (NLRB).[170]

Employers must be cognizant of striking the appropriate balance between allowing a reasonable use of the Internet for approved personal endeavors (particularly in regard to

---

[168] Content Technologies at www.mimesweeper.com.
[169] *Id.*
[170] Issues involving the NLRB are beyond the scope of this particular article; however, it should be noted that a complete prohibition of all personal use of computers and e-mail may be unlawful, especially if the employee was engaged in a "concerted activity" which is protected by the National Labor Relations Act. Sharon C. Zehe, *Beware Abridging E-Speech: Blanket Bans on Personal E-Mail and Internet Use at Work Can Lead to Trouble—For Employers,* MINNEAPOLIS STAR TRIB., July 24, 2000, Metro Edition, at D-3.

salaried employees who already work long hours) and monitoring employee Internet abuse, which could trigger additional litigation. Employee misuse of the Internet involves both complex management and legal issues such as: unfair work loads caused by cyberloafers, the impact of disclosure on whistleblowers, employees' expectations of privacy, and the right for employees to engage in "concerted activities."

The Internet issues discussed in this paper should not be taken lightly by employers or employees. Thus, given the potential liability involved, employers would be wise to draft an Internet use policy that specifically identifies "where voyage is forbidden!"