JULY/AUGUST 2001
VOLUME NO. 5 ISSUE NO. 7/8

FEATURE AND KEYCASE

ELECTRONIC INTERACTION IN THE WORKPLACE: MONITORING, RETRIEVING AND STORING EMPLOYEE COMMUNICATIONS IN THE INTERNET AGE

By Mark S. Dichter and Michael S. Burkhardt

INTRODUCTION

A. USE OF ELECTRONIC MAIL AND THE INTERNET IN THE WORKPLACE

A 1998 survey conducted by Forrester Research, Inc. estimates that 98%of all companies with more than 1,000 employees have Internet access and 45% of businesses with 20 to 99 employees are online. (1) According to International Data Corp., as of the end of 1998, 90 million United States workers were sending 1.1 billion business e-mail messages per day. By the year 2000, IDC projects that 130 million workers will flood recipients with 2.8 billion such messages each day.(2) The number of users accessing the Internet continues to grow exponentially. According to a January 1998 report by Datamonitor, entitled, "The Future of the Internet," this global Internet population will reach 250 million in 2002 and 300 million in 2005.(3)

B. WHAT IS THE INTERNET

The Internet is a worldwide system of interconnected computers.(4) One component of the Internet is effectively a worldwide electronic mail system. In addition, the Internet is a vast compository of information that generally can be accessed easily by an Internet user. The Internet allows users to transmit text, data, computer programs, sounds and visual images worldwide quickly.

Unlike e-mail on a local or internal company network, e-mail sent on the Internet is not routed through a central control point and, in fact, it can take many and varying paths before reaching the recipients. In addition, e-mail on the Internet is generally not secure and can be viewed by intermediate computers between the sender and the recipient, unless the message is specially encrypted.

The ease with which messages can be exchanged over the Internet, of course, bears a price. One example of a cyberspace blunder demonstrates the potential dangers that come with this rapidly growing technology. The Philadelphia Inquirer, reported on May 8, 1999 that an FCC employee inadvertently sent a dirty joke entitled "Nuns in Heaven" to 6,000 journalists and government officials.(5) Instead of forwarding this joke to a friend, this employee who was responsible for sending out, by e-mail, the FCC's Daily Digest to these 6,000 individuals, mistakenly forwarded this joke to each person on the agency's distribution list. This mistake which resulted in embarrassment for the agency, not to mention possible discipline for the employee, shows how the single click of a mouse could send sensitive and confidential information to thousands of computer users and create serious problems for attorneys and their clients.

Individuals can exchange messages over the Internet on a particular topic of interest that are forwarded either automatically to recipients who are on a mailing list or through a moderator that oversees the distribution of the messages. In addition, there are discussion groups with no specific mailing lists or moderators. There are many commercial on-line services that provide their own "chat groups" including America OnLine, CompuServe, Microsoft Network, Prodigy, and AT&T Worldnet.

TORONTO INSURANCE CONFERENCE BLACK TIE DINNER
November 8 **Toronto, Ontario**
Contact: (416) 364-4000

TIWA BUSINESS MEETING
November 15 **Toronto, ON**
Contact Josie Fung at (416) 590-0038 x6951
Josie.fung@economicalinsurance.com

TORONTO INSURANCE CONFERENCE BLACK TIE DINNER
November 8 **Toronto, Ontario**
Contact: (416) 364-4000

QUOTABLE QUOTE

"According to the results of a 1998 SurfWatch survey, 24 percent of the time spent online by the employees of the participating companies was not work related. A March 1999 study, conducted by Worldtalk Corp., found that employees spend on average 30 minutes a day sifting through their deluge of e-mail messages."

Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age
Page 41

NetPartners estimated that businesses lost $450 million in worker productivity when Congress released the Starr Report and President Clinton's video deposition over the Internet.

The second category of Internet communication is the search for and retrieval of information located on remote computers. There are three primary methods to locate and retrieve information on the Internet: (1) file transfer protocol ("FTP"), which is a method of transferring one or more computer files from another computer; (2) searching through the resources available on a remote computer by using software search programs like Yahoo! or Alta Vista; and (3) searching the "World Wide Web."

The World Wide Web is a series of documents stored in different computers that display documents containing text images, sounds, animation and/or moving video. These documents generally contain "links" to other information or resources. An essential element of the World Wide Web is that every document has an address. Many organizations now have "home pages" on the Web.(6) Home pages are simply electronic documents that provide a series of links to other information. Each link automatically connects the user to that information and/or to another Web site on another computer connected to the Internet.

The Web runs on tens of thousands of individual computers on the Internet and has no centralized control. No single organization controls any membership in the Web, nor is there any single centralized point from which individual Web sites or services can be blocked from the Web. The only semblance of control or organization on the Web is that all information on the Web must be formatted in a certain way so that all users may read the material.

A survey conducted by Louise Harris and Associates, in February 1999, found that the most popular use of the Internet was e-mail with 63 percent of the respondents reporting that they send e-mails often.(7) SurfWatch Software, a division of Spyglass, Inc. launched CheckNet in March, 1998 to help companies determine how employees are using Internet access. According to the results of a 1998 SurfWatch survey, 24 percent of the time spent online by the employees of the participating companies was not work related.(8) A March 1999 study, conducted by Worldtalk Corp., found that employees spend on average 30 minutes a day sifting through their deluge of e-mail messages.(9)

Although sending and receiving e-mail accounts for a significant percentage of the online time spent by workers, exploring the Internet also preoccupies parts of the workday. SurfWatch determined that the three categories accounting for the largest portions of non-work surfing were general news, sexually explicit material, and investment information.(10)

The issues of explicit material and wasted time merged in the case of the Starr Report. NetPartners estimated that businesses lost $450 million in worker productivity when Congress released the Starr Report and President Clinton's video deposition over the Internet.(11)

C. Electronic Monitoring of E-Mail

According to preliminary data from the American Management Association, as of the first quarter of 1999, nearly 30 percent of major U.S. companies currently monitor employee e-mails, up from 20 percent in 1998 and 15 percent

in 1996.(12) Content Technologies, Inc., a company whose software reads incoming and outgoing messages, has seen its sales double every year from 1996 through 1998.(13)

Through March of 1999, AMA found that 84 percent of the participating companies inform their employees of their communication monitoring policy.(14) The financial sector, including banking, brokerage, and insurance companies are most likely to monitor their employees' communications, according to AMA.(15)

The enormous increase in electronic communications and surveillance potentially exposes employers to various forms of legal liability. Corporate decision-makers must thus decide what policies they wish to adopt concerning access to, use, and disclosure of electronic and voice mail sent and received by their employees on office communication systems. While varying significantly from company to company and jurisdiction to jurisdiction, the following issues should be considered:

1. Employee privacy rights.
2. The disclosure of confidential information.
3. The rights of third parties to obtain access to company records and the company's need to manage its resources.
4. The right of unions to access company employees via e-mail.

Many employers have failed to address these concerns by establishing an e-mail policy, and recent legal developments underscore the folly of such inaction. Now more than ever, it is imperative for employers to have a company e-mail policy in place. Still, to date, a significant number of companies do not have e-mail or Internet use policies in place. According to a study by International Data Corp., as of the end of 1998, sixty percent of the companies surveyed did not have an employee e-mail or Internet usage policy, while 25 percent said they had a general ban on personal use of those resources.(16)

Courts generally consider electronic surveillance, such as telephone monitoring, an "intrusion" sufficient to establish that element of the tort.

EMPLOYERS' RIGHTS TO MONITOR OR ACCESS EMPLOYEES' ELECTRONIC COMMUNICATIONS VERSUS EMPLOYEES' PRIVACY RIGHTS

An employee's right to e-mail privacy is largely governed by state tort law. There are four distinct torts protecting the right to privacy: (1) unreasonable intrusion upon the seclusion of another; (2) misappropriation of another's name or likeness; (3) unreasonable publicity given to another's private life; and (4) publicity that unreasonably places another in a false light before the public. See Restatement (Second) of Torts 652A.

The tort most relevant to e-mail interception by employers is the unreasonable intrusion upon the seclusion of another. Section 652B of the Restatement (Second) on Torts defines Intrusion upon Seclusion as intentionally intruding, physically or otherwise, upon the solitude or seclusion of another or his/her private affairs or concerns. Liability under this tort does not require that the information acquired be publicized or used by the employer. Id, Comment a. However, to establish the tort, the intrusion must be highly offensive to a reasonable person. Courts generally consider electronic surveillance, such as telephone monitoring, an "intrusion" sufficient to establish that element of the tort. Courts generally consider electronic surveillance, such as telephone monitoring, an "intrusion" sufficient to establish that element of the tort. See, e.g., *Billings v. Atkinson,* 489 S.W.2d 858 (Tex. 1973); *Nader v. General Motors Corp*., 255 N.E.2d 765 (N.Y. 1970) (telephone wiretapping). In determining the offensiveness of the intrusion, courts examine "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion, as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded. See Miller v. National Broadcasting Co., 232 Cal. Rptr. 668, 679 (Cal. Ct. App. 1986). While express or implied consent is one defense to liability, the mere good faith belief that consent has been given is normally not a defense.

In deciding whether an intrusion invades a private matter, courts require both that the employee has a subjective expectation of privacy and that the expectation be objectively reasonable. State courts responding to such tort claims have generally attempted to balance an employee's reasonable expectation of privacy against the employer's business justification for monitoring. Thus, the critical issues to examine when determining employer tort liability for monitoring or intercepting employee e-mail messages are: (1) does the plaintiff have a reasonable expectation of privacy and, if so, (2) was there a legitimate business justification for the intrusion sufficient to override that privacy expectation.

a) Cases Involving the Interception or Monitoring Of E-Mail

In one of the first cases to address the privacy rights of employees with respect to e-mail messages the federal district court applied Pennsylvania state law. *Smyth v. The Pillsbury Co*., 914 F.

Supp. 97 (E.D. Pa. 1996). In Pillsbury, the plaintiff, Michael A. Smyth, was an at-will employee who received certain e-mail messages on his home computer from his supervisor over defendant's e-mail system. He then exchanged e-mails with his supervisor, which contained offensive references and threats concerning the company's sales management. Specifically, the messages referred to the sales management and made threats to "kill the backstabbing bastards" and referred to the holiday party as the "Jim Jones Koolaid affair." Id. at 99 n.1. Company executives, who saw a printout of this message, then read all of his e-mail messages and terminated him for "inappropriate and unprofessional comments over Defendant's e-mail system." 913 F. Supp. at 98.

The plaintiff filed a wrongful discharge action alleging that the employer's conduct violated Pennsylvania's public policy protecting his right of privacy. The plaintiff argued that the interception of his e-mail messages was an impermissible intrusion upon seclusion. In support of his claim, the plaintiff alleged that the employer had repeatedly assured its employees that all e-mail communications would remain confidential and privileged. Id.

The court, taking a broad approach, found that there is no reasonable expectation of privacy in e-mail communications voluntarily made to a supervisor over a company-wide e-mail system despite the fact that the employer assured the plaintiff that the e-mail messages would not be intercepted by management. The court stated:

> Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system, which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.

914 F. Supp. at 101. The court went on to decide that even if there was a reasonable expectation of privacy, a reasonable person would not consider the employer's interception to be a substantial and highly offensive intrusion upon seclusion. Id. Finally, the court held that the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighed any privacy interest the employee may have had in his comments. Id.

In *Bohach v. Reno,* 932 F. Supp 1232 (D.Nev. 1996), the court denied plaintiffs' application for a preliminary injunction based on alleged violations of the Reno police department's monitoring alphanumeric pager messages which the plaintiffs, who were police officers, sent to each other over the department's message system. The police officers had been told that all messages would be logged on the network and that the system should not be used for certain types of messages. The system was also freely accessible with no password requirement. The court held that the system was essentially electronic mail and that the officers did not have an objectively reasonable expectation of privacy in these communications and therefore were not likely to prevail on their Fourth Amendment civil rights claim.(17)

The California Court of Appeals also upheld an employer's right to access employees' e-mail. In *Bourke v. Nissan Motor Corp.*, No. BO68705 (Cal.Ct. App. July 26, 1993) (unreported decision),(18) defendant Nissan conducted training seminars about the use of its e-mail system in which a trainer randomly accessed an e-mail message for demonstration purposes. The e-mail message, written by the plaintiff, contained information of a personal, sexual nature. After the incident was reported to management, the plaintiff's e-mail messages and those of others in her work group were reviewed. Several employees received written warnings as a result.

The plaintiff and one other employee, who was ultimately fired, sued Nissan for invasion of privacy, violation of criminal wiretapping statutes, and wrongful discharge. The appellate court affirmed the trial court's grant of summary judgement in favor of Nissan holding that the plaintiffs had no reasonable expectation of privacy in their e-mail messages because they had signed a waiver form stating that it was company policy that employees restrict their use of company-owned computer hardware and software to company business.(19) In addition, the court determined that the plaintiffs had no reasonable expectation of privacy because, many months before their terminations, they learned that their e-mail messages were periodically read by employees other than the intended recipients.(20) The plaintiffs next attempted to argue that they had a privacy expectation because they were given passwords to access the system and were told to safeguard their passwords, but the court held that such a claim did not raise a question of law as to whether their expectations were objectively reasonable.(21)

The plaintiffs had no reasonable expectation of privacy in their e-mail messages because they had signed a waiver form stating that it was company policy that employees restrict their use of company-owned computer hardware and software to company business.

The cases of *Shoars v. Epson America, Inc.*, No. BO73243 (District, Div. 2), review denied, No. SO40065, 1994 Cal. LEXIS 3670 (1994)and *Flanagan v. Epson America, Inc*., No. BC007036 (Super. Ct. L.A. Co., Jan. 4, 1991) offer additional possible support for an employer's right to monitor e-mail messages.(22) In *Shoars*, Alana Shoars was responsible for providing employees with training and support in the use of the office e-mail and she informed employees that their messages were confidential. Upon discovering that her supervisor had been intercepting and reading all e-mail messages entering and leaving the office, Shoars demanded that he stop. When she sought an e-mail account number to which her supervisor could not access, she was fired for gross insubordination. Shoars sued Epson under California Penal Code Section 631. The California statute provided a private cause of action for illegal interception of private telegraph and telephone wire communications. In Flanagan, about 700 Epson employees brought a class action suit against the company under Section 631, Flanagan, No. BO07036, Slip op. at 1-2. The court rejected class certification for this second case shortly thereafter.(23)

The Shoars court rejected Shoars' claim that Epson's actions constituted a violation of Section 631 because the court was unwilling to extend the statute's protections to cover electronic communications. The Flanagan court reached the same conclusion, but stated it was not clear that the employees had an expectation of privacy, which was a required element for an invasion of privacy action.

B. Other Analogous Case Law Involving Workplace Searches Or Surveillance

Other analogous case law involving workplace searches can provide some guidance in this area. Perhaps the most analogous context involves searching employees' lockers and desks. An employer searches an employee's e-mail file for relevant data or for messages documenting suspected wrongdoing much in the same way as an employer would search an employee's desk for either a missing file or documents indicating employee wrongdoing.

Perhaps the most analogous context involves searching employees' lockers and desks. An employer searches an employee's e-mail file for relevant data or for messages documenting suspected wrongdoing much in the same way as an employer would search an employee's desk for either a missing file or documents indicating employee wrongdoing.

For example, in *O'Bryan v. KTIV Television,* 868 F. Supp. 1146 (N.D. Iowa 1994), aff'd in relevant part, 64 F.3d 1188 (8th Cir. 1995), the court held that a plaintiff failed to state a common law invasion of privacy claim arising out of an alleged search of his desk. The O'Bryan court stated that even if the employer had in fact searched the employee's desk, the plaintiff failed to show that, given the operational reality of the workplace, he had a reasonable expectation of privacy in the contents of his desk or credenza, neither of which were locked and both of which contained marketing information that would be needed by other employees. 864 F.Supp. at 1159. However, the court noted that searching an employee's work space may constitute a tortious invasion of privacy if the search is conducted in such a way as to reveal information unrelated to the workplace. Id. Another court reached a similar conclusion. See *Doe v. Kohn, Nast & Graf,* 862 F.Supp. 1310 (E.D. Pa. 1994). John Doe, an attorney infected with the HIV virus, sued his former law firm for various claims including for invasion of privacy. Allegedly, a partner in his former law firm searched his office and discovered a letter from his doctor relating to his HIV status. The court found that a search of an employee's work area that is done in such a way to reveal matters unrelated to work, may constitute an invasion of privacy and determined that the issue was properly left up to a jury. 862 F. Supp. at 1326.

In *K-Mart Corp. Store No. 7441 v. Trotti,* 677 S.W.2d 632 (Tex. Ct. App. 1984), however, the court found the employer liable for $100,000 in punitive damages for searching an employee's locker on the mere suspicion that the employee had stolen goods from the store. The court appeared to rely on the fact that the employee had purchased and used her own lock to support a reasonable expectation of privacy. However, if that is sufficient, then employees everywhere could establish a reasonable expectation of privacy by locking their materials with their own locks. Applying this approach to e-mail, a court might conclude that an e-mail password or e-mail software denying access to outsiders could support a reasonable expectation of privacy.

It is apparent that the particular employment setting will determine whether an employee has a "reasonable expectation of privacy." A 1999 state court in Texas considered whether an e-mail password could support a reasonable expectation of privacy. In May 1999, the Texas Court of Appeals considered whether a cause of action should be recognized for invasion of privacy based on an employer's review and dissemination of electronic mail stored in a "personal folders" application on an employee's office computer. The Court of Appeals of Texas, in an

unpublished opinion, affirmed the trial court's determination that the employee had failed to allege facts sufficient to state a cause of action for invasion of privacy. *McLaren v. Microsoft Corp.,* 1999 WL 339015 (Tex.App.-Dallas), The employee claimed that the fact that his e-mail messages were stored under a private password with the employer's consent gave rise to a legitimate expectation of privacy. In upholding the district court, the Court of Appeals found that the employee's computer was provided to him by the employer so that he could perform the functions of his job; therefore, the messages contained on the computer were not his personal property but merely an inherent part of the office environment. The Court held that the employee, even by creating a personal password, did not manifest a reasonable expectation of privacy.

In McLaren, the Court, considering the holding in Trotti, distinguished the privacy interest an employee may have in his personal locker with the interest he may have in his computer. The Court found that the nature of the locker and an e-mail storage system are different. The Court noted that a locker was a discrete, physical place where an employee could store his personal effects separate and apart from other employees. On the other hand, the Court recognized that any e-mail messages that the employee places in his personal folder were first transmitted over the network and were at some point accessible to third parties.

It is possible, however, that if the e-mail messages are encrypted or coded so that only the sender and the recipient can read the messages, a further expectation of privacy may be created. Absent a policy explaining that e-mail messages are not private, or explaining that the employer can gain access to e-mail despite a personal password, an employer is at greater risk that a court may find that the employee had a reasonable expectation of privacy with respect to his/her e-mail messages.

Absent a policy explaining that e-mail messages are not private, or explaining that the employer can gain access to e-mail despite a personal password, an employer is at greater risk that a court may find that the employee had a reasonable expectation of privacy with respect to his/her e-mail messages.

Assuming an employee has a reasonable expectation of privacy in his or her e-mail message, courts will inquire into the purpose for the interception. Courts, have found that an employer's legitimate business interest can justify invasive conduct. See *Smyth*, 914 F. Supp. at 101 (company has strong interest in preventing inappropriate and unprofessional e-mail communications and that interest outweighs any privacy interest). See also *Saldana v. Kelsey-Hayes Co.*, 443 N.W.2d 382, 384 (Mich. Ct. App. 1989) (concluding that employer's legitimate business interest in investigating the employee's claim of work-related injury outweighed employee's privacy interest in not being monitored in his home);

Simmons v. Southwestern Bell Tel. Co., 452 F. Supp. 392, 394 (W.D. Okla. 1978) (employer who monitors telephone calls in effort to ensure quality control and who provides employee notice of such monitoring satisfies reasonable conduct requirement), aff'd, 611 F.2d 342 (10th Cir. 1979).

C. Analogous Case Law Involving Public Employers

In contrast to private employers, public employers are constrained by the Fourth Amendment of the United States Constitution. The Fourth Amendment that is applied to the states through the Fourteenth Amendment, protects individuals from unreasonable searches and seizures.

A public employer must balance its employees' constitutional rights and reasonable expectations of privacy against its own interest in conducting the search. See *O'Connor v. Ortega*, 480 U.S. 709 (1987). Applying this principle, the Supreme Court held that public-sector workplace searches are constitutional if they are tailored to the government's interest in the efficient and proper operation of the job site. Id. at 723. In the landmark case, O'Connor v. Ortega, the Supreme Court applied those principles to the employment context.

The privacy claim in *Ortega* stemmed from a state hospital official's search of the office, desk, and file cabinet of a physician suspected of mismanagement of the hospital's residency program. Id. at 712-13. In determining the propriety of the search, the Court held that both the inception and scope of employee searches and surveillance are to be judged according to a case-by-case reasonableness standard "under all [the] circumstances." Id. at 725-26. Under this reasonableness standard, Fourth Amendment rights are violated only if public employees have an expectation of privacy that society is prepared to recognize as reasonable. The Court noted, however, that this privacy expectation "may be reduced by virtue of actual office practices and procedure, or by legitimate regulation." Id. at 717. The *Ortega* Court determined that a search conducted by a public employer is reasonable when the employer offers legitimate business reasons (such as the employer's need for supervision, control, and efficiency in the workplace)

Findings of probable cause and warrants are not required for public employer searches conducted either for work-related, non-investigatory reasons, or for investigations of work-related employee misconduct.

for the search such that its needs outweigh the employee's protected privacy interests. Id. at 719-20. In Ortega, the Court found that Dr. Ortega had a reasonable expectation of privacy in his desk and file cabinets because both of those items were located in his office and the hospital had seized personal items from his desk and file cabinet. 480 U.S. at 718. Significantly, the Court found that Dr. Ortega's desk contained personal information such as personal correspondence, medical files, correspondence from private patients unconnected to the hospital, personal financial records and personal gifts. Id.

Thus, based on Ortega, public employers have generally been granted wide latitude to search employee work areas and personal effects, including the employee's computer. In The *United States v. Mark L. Simons*, 29 F. Supp.2d 324 (E.D.Va. 1998), the court denied defendant's motion to suppress evidence obtained from his office computer. Defendant, a CIA employee, who had access to the government computer system as well as the Internet, was indicted on two counts of receiving and possessing material containing child pornography. The court, in consideration of the employer's Internet policy which authorized audits to support the identification, termination and prosecution of unauthorized activity, held that the defendant did not have a reasonable expectation of privacy with regard to any Internet use at work. 29 F. Supp.2d at 328. See also *Williams v. Philadelphia Hous. Auth.*, 826 F. Supp. 952 (E.D. Pa. 1993) (searching absent employee's office for computer disk containing work-related material, even though disk also contains personal information, held to be reasonable and based on legitimate business need); *American Postal Workers Union v. United States Postal Serv.*, 871 F.2d 556 (6th Cir. 1989) (union contract permitted locker searches); *Chicago Fire Fighters Union, Local 2 v. City of Chicago*, 717 F. Supp. 1314 (N.D. Ill. 1989) (job regulations stated that employee lockers were subject to search). See also *Melton v. United States Steel Corp.*, 8 Indiv. Empl. Rights Cas. (BNA) 687 (N.D. Ill. 1993) (legitimate reason to search employees where company policy banned drug use)

Findings of probable cause and warrants are not required for public employer searches conducted either for work-related, non-investigatory reasons, or for investigations of work-related employee misconduct. *Ortega* , 480 U.S. at 725. Moreover, if employees are notified concerning the types of searches that may be conducted and the areas that may be searched, their reasonable expectations of privacy in those areas are reduced. See, e.g., *United States v. Bunkers*, 521 F.2d 1217, 1221 (9th Cir.) (postal employee's use of locker with understanding that employer would conduct searches upon reasonable suspicion was "effective relinquishment" of her Fourth Amendment immunity), cert. denied, 423 U.S. 989 (1975); *McDowell v. Frank*, No. C-91-0358-DLJ, 1992 U.S. Dist. LEXIS 16863 p.3 (N.D. Cal. Oct. 16, 1992) (employee knowledge of collective bargaining agreement provision permitting locker searches and continued searches of locker prevented a finding that the employee had a reasonable expectation of privacy in locker). See also *Sheppard v. Beerman*, 822 F. Supp. 931 (E.D.N.Y. 1993) (upholding warrantless search of former law clerk's desk and file cabinets where a clerk had no reasonable expectation of privacy in desks, file cabinets or other work areas, which mostly contained court case files and memoranda), aff'd in relevant part, vacated in part, 18 F.3d 147 (2d Cir. 1994), cert. denied, 115 S. Ct. 73 (1994).

In addition, cases involving vehicle searches are also analogous. An employee's expectation of privacy in a vehicle is less than it is with other property. Nevertheless, in cases involving searches of an employee's vehicle by a public-sector employer, courts will balance the employee's reasonable expectation of privacy against the employer's need to conduct the search. For example, in *McDonell v. Hunter*, 809 F.2d 1302, 1309 (8th Cir. 1987), the court held that a correctional institution's search of vehicles without cause was reasonable, because the vehicles, which were parked at the facility were accessible to inmates. The only caveat added by the court was that the searches must be conducted uniformly or by a systematic random selection. 809 F.2d at 1309.

In the *United States v. Charboneau*, 979 F. Supp 1177 (S.D. Ohio 1997),

However, e-mail messages, like a letter, cannot be afforded a reasonable expectation of privacy once that message is received.

A 1997 study concluded that more than 30 percent of all e-mail messages sent by employees concerned nonwork-related topics.

the court considered whether the FBI had violated defendant's Fourth Amendment rights by monitoring the e-mail messages sent by defendant to a child pornography "chat room." The court held that the transmitter of e-mail enjoys a reasonable expectation of privacy that the police will not intercept transmission without probable cause and a search warrant. However, e-mail messages, like a letter, cannot be afforded a reasonable expectation of privacy once that message is received. 979 F. Supp at 1184. Similarly, an e-mail message sent to the public at large in a "chat room" loses any semblance of privacy. 979 F. Supp at 1185.

The Fourth Amendment's protection against unreasonable search and seizure may be relevant to private sector employers who monitor employee communications over e-mail. Fourth Amendment rights apply to private sector employees when the private employer acts under the color of federal or state law as a result of the direction of government regulation or law enforcement officials. See *Skinner v. Railway Labor Executives' Ass'n.*, 489 U.S. 602, 614-16 (1989)(holding Fourth Amendment applicable to drug testing conducted by private employers pursuant to government regulations). Furthermore, constitutional provisions may also apply to private employers that act as governmental bodies or substantially undertake governmental functions. See, e.g., *Marsh v. Alabama*, 326 U.S. 501 (1946)(private corporation which essentially acted as municipality in company-owned town considered state actor).

EMPLOYER LIABILITY BASED ON EMPLOYEES' USE OF ELECTRONIC MAIL

A 1997 study concluded that more than 30 percent of all e-mail messages sent by employees concerned nonwork-related topics.(24) Many employees erroneously assume that their electronic messages are private and will be deleted automatically upon their command. However, these assumptions are wrong and use of e-mail messaging services for careless, inappropriate, defamatory, or even offensive communications may later expose them and their company to significant litigation liability. Wrongful termination based on discrimination, sexual harassment, and breach of privacy have all been alleged by recent plaintiffs. Recent case law in this area illustrates this point:

In Seattle, a woman sued her former employer for age discrimination after she was fired. Her complaint seemed unlikely to succeed — at least initially — as the company's termination letter was "picture perfect by human resources standards." (25) During the discovery process, however, plaintiff's attorney hired a computer consultant specializing in e-mail retrieval. This consultant used sophisticated software to "unerase" a supposedly deleted e-mail message from the company's president to the head of the personnel department. The president's e-mail had instructed the supervisor to "get rid of the tight-assed bitch."(26) Faced with this evidence, the company's attorney, who had previously viewed the case as nothing more than a nuisance, suddenly agreed to settle for $250,000.

Likewise, in another case, four female employees sued Microsoft for sexual harassment where the alleged sexual harassment included a number of pornographic e-mail messages sent between employees at the company's information and technology division. (27) Although it denied the charges, this company quickly settled the lawsuit for $2.2 million plus the plaintiffs' attorneys' fees and court costs.

A. The Smoking Gun E-Mail

Courts have relied upon e-mail messages as important evidence in numerous cases. In their antitrust suit against Microsoft Corp., the Justice Department introduced dozens of internal e-mail messages. The Justice Department has attempted to prove that Microsoft has used illegal tactics over the past three years to overtake Netscape Communications Corp. in the browser market. The government lawyers introduced one e-mail message from Chairman William Gates to some Microsoft executives regarding a Gates' attempt to convince Intuit Chief Executive Scott Cook to switch from Netscape's browser to Microsoft's browser. Gates wrote, "I was quite frank with him that if he had a favor we could do for him that would cost us something like $1 million to do that in return for switching browsers in the next few months I would be open to doing that." While the government characterized this communication as a bribe, Microsoft explained that they were simply compensating Intuit for the expense involved in switching from Netscape's software.(28)

In In re *Air Disaster at Lockerbie, Scotland,* 37 F.3d 804, 815-816 (2d Cir. 1994), the court upheld a jury verdict in favor of plaintiffs against PanAmerican World Airways, Inc. and upheld the trial court's ruling that an e-mail message was admissible.(29) Various families of the victims of the air disaster over Lockerbie, Scotland filed wrongful death actions against PanAm. Their damages would have been limited to $75,000 unless they could prove wilful misconduct on behalf of PanAm. The FAA had instituted very strict regulations governing security at various airports including Heathrow Airport in London, England. One of the regulations required that all unaccompanied

bags be physically searched in addition to being x-rayed. Despite that regulation, the director of PanAm Security sent an e-mail message to all regional security representatives stating that they did not have to use x-ray and personal searches. In reality, although PanAm could have sought an exemption to the regulation, they in fact never formally requested such an exemption in writing as was required by the regulations. Thus, the e-mail message introduced by plaintiffs was extremely helpful in ultimately proving the existence of wilful misconduct on the part of PanAm and the jury awarded approximately $20 million to three families in that case.

Similarly, discovery requests for computer information can often lead to the recovery of old e-mails, prior versions of documents, employer's motives and private assessments of an individual employee. See *Siemens Solar Indust. v. Atlantic Richfield Co.*, Civ. A. No. 93-Civ-1126 (LAP) 1994 U.S. Dist. LEXIS 3026 (S.D.N.Y. Mar. 16, 1994). E-mail messages sent by Arco employees were retrieved from a computer system of an Arco subsidiary that was acquired by Siemens in 1990. These e-mails demonstrated that Arco employees concealed serious flaws with the commercial viability of the subsidiary's thin film silicon (TFS) technology when the company was sold to Siemens. In fact the court found that the e-mail messages made it clear that, prior to the sale, ARCO employees were aware that production of TFS was not commercially viable.

E-mail messages that are "deleted" (i.e., clicking on a delete button with his/her mouse) may not necessarily be inaccessible or unretrievable. Consequently, "deleted" e-mail messages may still be subject to a discovery request. Specifically, if information that has been "deleted" has yet to be overwritten by the computer system or is stored on backup tapes or archive tapes, the information may still be accessible.(30) For example, deleted e-mail messages played a key role in exposing the Iran-Contra Affair when the deleted e-mail messages from the White House were retrieved from a mainframe back-up tape. See *United States v. Poindexter*, Crim No. 88-0080-01 (HHG) 1990 U.S. Dist. LEXIS 6173, at *12, n.12 (D.D.C. May 29, 1990) (referring to White House Prof Notes, which was a form of electronic mail, as evidence supporting the conspiracy allegation)

The e-mail message introduced by plaintiffs was extremely helpful in ultimately proving the existence of wilful misconduct on the part of PanAm and the jury awarded approximately $20 million to three families in that case.

B. E-mail Constituting Racial Harassment

In several cases courts have addressed claims that e-mails constituted racial harassment. In Curtis v. Dimaio, 1999 WL 224603 (E.D.N.Y.), plaintiffs alleged that Citibank managers circulated racial and ethnic jokes over the e-mail system at work. According to the court, the discriminatory conduct involved the e-mail transmission of a Polish joke and an Ebonics joke. The district court, in dismissing the complaint, held that hostile work environment claims are meant to protect individuals from abuse and trauma that is severe. They are not intended to promote or enforce civility, gentility or even decency. As such, a claim that "my co-worker is unpleasant" or event that "my co-worker is a racist" without more will not support a claim for a hostile work environment. 1999 WL 224603, *7.

In *Daniels v. WorldCom Corp*., 1998 WL 91261 (N.D.Tex.), two WorldCom, Inc. employees alleged that they were racially discriminated against while working at defendant WorldCom, Inc. The plaintiffs assert that four e-mails received from a non-managerial employee were racially harassing. After receiving the complaint from plaintiffs, the Human Resources Manager took immediate action which included issuing a strong verbal warning to the sender and placing a written reprimand in her personnel file. The manager's actions also included the holding of two staff meetings, one where the employees were reminded not to use the e-mail system for non-business purposes and one where the employees were allowed to voice their displeasure about the e-mails. Finally, the manager initiated a review of the company's e-mail policy. 1998 WL 91216, at *1. Although the plaintiffs' claims were dismissed for failing to exhaust administrative remedies, it is significant that the court took note of the employer's prompt remedial action which included disciplining the individual who violated the company's e-mail policy.

In *Owens v. Morgan Stanley & Co.*,Inc., 1997 WL 793004 (S.D.N.Y.), two African-American employees claimed that they were discriminated against after they complained about receiving an e-mail message containing a racist joke. In late 1997, a federal judge in New York ruled that the plaintiffs could proceed with their $60 million suit against the investment banking firm. In early 1998, both sides reached a confidential settlement.

C. E-mails Constituting Sexual Harassment

One problem facing employers is so-

An Ohio jury found that a female employee was sexually harassed and subject to a hostile work environment because she could see the pornographic pictures that her male co-worker had downloaded off the Internet. The jury awarded the plaintiff $265,000 in damages.

called unwelcome e-mail messages and the creation of a sexually hostile work environment through the use of e-mail and the Internet. Because of the prevalence of e-mail in the workplace and the ability to easily forward e-mails to a larger number of employees, employers must be aware of what their employees are saying and doing with e-mail. In addition, because sexually explicit material is readily available from the Internet, and this material can be easily downloaded and forwarded to other employees, employers must be especially cognizant of hostile work environment claims involving the viewing and transmitting of sexually explicit information in the workplace.

The extent to which an employer may be held liable for a sexual harassment claim based on e-mail messages or sexually explicit Internet material generally depends upon the severity and pervasiveness of the conduct, the employer's knowledge and the employer's response. There are many examples of how misuse of e-mail or the Internet can lead to employer liability. For example, a subsidiary of Chevron Corporation had a list "why beer is better than women" circulated throughout the company on its e-mail system. The hostile work environment sexual harassment claim was filed based on that e-mail. The claim was settled out of court for $2.2 million.(31)

In *Schwenn v. Anheuser-Busch, Inc.*, 1998 WL 166845 (N.D.N.Y.), an employer filed a claim for sexual harassment against her employer after receiving sexually harassing e-mail messages, over a three-week period, on her computer terminal at work. Plaintiff testified that she received e-mails stating, "I want to eat you" and "meet me in aisle 50 [at a specific time]." Upon receiving the employee's complaint, the supervisor immediately conducted two meetings with warehouse workers in which he informed them of the complaint, reiterated the policy against sexual harassment, which included harassment via e-mail, and informed them that the company would audit the e-mails. The court held that the plaintiff failed to prove that the actions of her co-workers were sufficiently severe or pervasive enough to create a hostile work environment and granted defendant's motion for summary judgment. 1998 WL 166845, at *4. The court did not find three weeks of harassment to be pervasive enough to warrant a hostile environment claim.

In *Trout v. City of Akron*, an Ohio jury found that a female employee was sexually harassed and subject to a hostile work environment because she could see the pornographic pictures that her male co-worker had downloaded off the Internet.(32) The jury awarded the plaintiff $265,000 in damages.

In *Harley v. McCoach*, 928 F. Supp. 533 (E.D. Pa. 1996), an employer, also, faced a claim of sexual harassment that involved the use of e-mail. The plaintiff in Harley worked in a warehouse and was one of two women in the entire warehouse. In addition to a tremendous amount of sexual conduct, the court reviewed an e-mail message sent to the Plaintiff identifying her as "Brown Sugar." After the plaintiff complained, and an investigation was conducted, the employer instituted remedial measures, which included removal of electronic mail capability from the warehouse. 928 F. Supp. at 535. Despite the fact that the Employer took away e-mail privileges, the court found a genuine issue of material fact as to whether the employer took prompt and remedial action upon learning of the harassment. 928 F. Supp. at 540.

Employers can also face litigation from employees who they terminate for improper use of e-mail. For example, in *Donley v. Ameritech Services*, Inc., 1992 U.S. Dist. LEXIS 21281 (E.D. Mi. Nov. 16, 1992), Plaintiff sent an e-mail message to a female co-worker referring to an African American male client as "John Webb the Turd," and by replacing all of the "th's" with "t's" in his message and the "the's" to "ta's." Upon receipt of the message, the female co-worker complained to her Caucasian, female supervisor and the plaintiff was later discharged for sending an e-mail which was offensive and disrespectful to the client. Plaintiff argued that Ameritech discriminated against him on account of his race (Caucasian) and defamed him during his discharge. The court granted summary judgment in favor of Ameritech on the grounds that the plaintiff had failed to establish a prima facie case of reverse discrimination and the lack of a genuine issue of material fact on whether the e-mail incident was a pretext for intentional discrimination against the plaintiff.

D. Defamation

One area of potential concern for employers is potential liability for defamatory statements sent out on an employer's e-mail system or posted on an employer's home page or electronic bulletin board. Recent case law and

legislation have helped to clarify what has been a controversial issue. In May 1995, the New York Supreme Court, in *Stratton Oakmont, Inc. v. Prodigy Services Co.*, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), considered whether an on-line computer service could be held liable for defamatory statements posted through its service. Following an allegedly libelous posting on one of Prodigy's bulletin boards in 1994, Stratton Oakmont brought a defamation suit against Prodigy Services Co. When Prodigy began in 1990, it held itself out as a family service where it would not permit obscenity or insulting conduct on its bulletin boards. However, because of the enormous increase in the use of Prodigy's bulletin boards, Prodigy abandoned its content monitoring and simply used a software screening program that automatically prescreens certain offensive language. In 1994, an unidentified individual, using an identification code of a Prodigy employee, posted statements on one of Prodigy's bulletin boards that Stratton Oakmont and its President had committed criminal and fraudulent acts in connection with a public offering and called Stratton a "cult of brokers who either lie for a living or get fired." 1995 WL 323710, at *1. Whether Prodigy was responsible for the defamatory statements and the applicable standard of truth centered around the issue of whether Prodigy was the "publisher" of the information or merely a distributor of the information. The court in Stratton Oakmont found that Prodigy was a publisher because it exercised some editorial control over materials that were published on its bulletin boards. Thus, the court applied the standard that Prodigy as a publisher would be strictly liable for any materials it published on its bulletin boards.

In 1996, Congress overruled the precedent established in Stratton Oakmont by enacting the "Good Samaritan" provisions of the Communications Decency Act, which created a federal defense to state law causes of action for defamation.(33) Although the Supreme Court struck down the indecency provisions of the Communications Decency Act as unconstitutional in *Reno v. ACLU,117 S.Ct.* 2329(1997), the "Good Samaritan" provisions were not at issue in Reno and remain in effect.

Attorneys must be wary of sending confidential information via external e-mail because of possible interception or "accidental e-mails."

Section 230(c) provides in relevant part:

- No provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another content information provider.
- No provider or user of an interactive computer service shall be liable on account of any action voluntarily taken in good faith to restrict access to or availability of objectionable material.
- No cause of action may be brought and no liability may be imposed under any state or local law that is inconsistent with this section.

Congress enacted section 230 to remove the disincentives to self regulation created by the Stratton Oakmont decision. Fearing that the specter of liability would therefore deter service providers from blocking and screening offensive material, Congress enacted this provision's broad immunity "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material." 47 U.S.C. 230(b)(4).(34)

Courts have broadly interpreted the language of section 230. In *Zeran V. America Online*, 129 F.3d 327(4th Cir. 1997), cert denied 118 S.Ct. 2341(1998), plaintiff alleged that AOL had unreasonably delayed in removing the defamatory messages posted by an unidentified third-party, refused to post a retraction, and failed to screen similar future postings. Plaintiff argued that section 230 of the Communications Decency Act left in tact liability for interactive service providers who possess notice of defamatory material posted through their services. 129 F.3d 327. The Fourth Circuit held that by its plain language section 230 creates a federal immunity to any cause of action that would hold service providers liable for information originating with a third party user of the service. Id., at 330. Specifically, section 230 precludes a court from entertaining claims that would place a computer service provider in a publisher's role. Id.

The Communications Decency Act was also relied upon in limiting claims against an Internet service provider. *Blumenthal v. Drudge*, 992 F. Supp 44 (D.D.C. 1998). This case concerned statements written by columnist Matt Drudge in "The Drudge Report" about White House aide, Sidney Blumenthal. America Online had contracted with Drudge to make his column available to AOL subscribers. When Drudge reported that Blumenthal was a wife-abuser, Blumenthal responded by filing an action for defamation against both Drudge and America Online. The court held that an interactive computer service provider could not be held liable for making an allegedly defamatory gossip column, written by another information content provider, available

to service provider subscribers, in absence of evidence that the service provider had some role in writing or editing material or creating or developing information in the column. 992 F. Supp. at 49.

DISCLOSURE OF CONFIDENTIAL INFORMATION

The very versatility and simplicity of e-mail undermines a company's ability to protect its trade secrets and other confidential information. A disgruntled employee, for example, could easily disseminate sensitive information to anyone connected to the e-mail network, including outside users, competitors, and future employers. Moreover, attorneys must be wary of sending confidential information via external e-mail because of possible interception or "accidental e-mails.(35)

An article in the September 1995 edition of the *ALAS Loss Prevention Journal* at p. 12, illustrates the dangers of engaging in electronic communications. The article discusses the case of a young lawyer communicating on an electronic bulletin board (Counsel Connect). The associate at a major law firm was engaged in a chat with several other attorneys and expressed some views that may not have been acceptable to the firm or the firm's clients. The associate identified the firm she was from, and the information eventually reached a partner in the firm. While the situation was simply embarrassing to the firm involved, it could have had other ramifications depending on the content of the message.

The article also points out that these lawyer chat groups raise serious issues of confidentiality and attorneys' ethical obligations vis-a-vis client confidences. Specifically, where an attorney presents a hypothetical on an electronic bulletin board seeking the advice of other attorneys, the attorney may still be running a risk of violating a client's confidences, because opposing counsel in the case may also have access to the bulletin board and instantly recognize

Corporate Email Policy Guidelines

The first step in professionalizing your email communications is to publish a corporate email policy. This email policy accomplishes three objectives:

1. Commercial objective: in teaching employees how to send effective emails and stating target answering times, you can professionalize your email replies and therefore gain competitive advantage
2. Productivity objective: by setting out rules for the personal use of email you can improve productivity, and avoid misunderstandings.
3. Legal objective: in clearly stating what is considered as inappropriate email content you can minimize the risk of law suits and minimize employer's liability by showing that the company warned employees about inappropriate email use.

What should be included in an email policy?

Commercial: guidelines on how to write effective emails

- Corporate email style (formal/informal). This could include guidelines on salutation and ending of messages.
- What kind of signatures should be used, i.e. should signatures include company name, job function, telephone & fax number, address, website and/or a corporate slogan.
- Basic rules on how to write email messages.
- Expected time in which emails should be answered. For example, you could set a general rule that each email should be answered within at least 8 working hours, but 50% of emails should be answered within 4 hours.
- How to determine which emails should receive priority.
- When to send cc: or bcc: messages and what to do when you receive them.
- How and when to forward email messages and how you should handle forwarded messages.

Productivity: rules on the usage of the email system

- Whether personal e-mails are accepted and if so, to what extent. For instance you could limit the amount of personal emails sent each day, or you could require personal emails to be saved in a separate folder. You could also limit or eliminate certain email attachments from being sent or received, and include rules on sending chainletters. Include examples and clear measures taken when these rules are breached.
- Use of newsletters & news groups. For instance you can require a user to request permission to subscribe to a newsletter or news group.

Legal: prohibit inappropriate email content and warn of risks

- Include a list of 'email risks' to make users aware of the potential harmful effects of their actions. Advise users that sending an email is a like sending a postcard: if you don't want it posted on the bulletin board, then don't send it. (For more information about the legal risks of email, visit emaildisclaimers.com)
- What kind of content is deemed unacceptable, for instance pornographic or libelous content. Include examples and clear measures taken when these rules are breached.

continued on page 54

continued from page 53

- If you are going to monitor the content of your employees' emails, mention this in your email policy. In most countries/states you are allowed to monitor your employees' emails if your employees are made aware of this.

Finally, include a point of contact for questions arising from the email policy.

Publishing the email policy

When you have formulated an email policy, you should make sure that all employees are aware of the policy. You can do this by handing out printed copies and publishing it on your intranet. Also, when a new employee starts at your company, this employee should be given a copy of the document as standard. It is also a good idea to include the most important points of the email policy in the employment contract. Cover for instance the personal use of email and possible email monitoring in the contract. Also mention that defamatory, sexual and racist remarks in emails are strictly forbidden and that such behavior can lead to termination of employment.

Furthermore, you could organize an email training to make sure that the policy is actually put into practice and everything is clear. Training is also useful for obtaining feedback to ensure that the policy is feasible and can actually be put into practice.

Updating the email policy

Since developments in email and the Internet are changing rapidly, it is important to review the email policy at least every quarter. Keep an eye on new developments in email and Internet law so that you are aware of any new regulations and opportunities.

This material reprinted with permission from www.emailreplies.com. For more on email policies see also: http://www.email-policy.com.

the hypothetical. Thus, attorneys must be careful when engaging in communications on electronic bulletin boards. See also discussion below at IV.B on ethical issues.

A. Trade Secrets

A search of an employee's e-mail messages may provide evidence of trade secret theft. Borland International suspected that a former employee who defected to a major competitor had been using the company's own e-mail system to transmit trade secret information to one of its major competitor's top executives, Gordon Eubanks. Information uncovered during the search confirmed these initial suspicions, and led to civil and criminal actions against the former employee and Eubanks.(36) They were both charged with 31 felony counts of criminal trade secret theft under California Penal Code Section 499c.(37) The criminal charges against both defendants were ultimately dismissed at the request of the Santa Cruz County District Attorney.(38)

The unauthorized disclosure of confidential information to third parties via electronic media should be strictly prohibited. Employees should be encouraged to report immediately any such incidents to the appropriate corporate personnel, and the company's overall written confidentiality policy should reflect these concerns. Lastly, employees should be reminded periodically not to leave e-mail messages on their screens when they leave their computers and to change their passwords frequently to avoid unauthorized access by hackers.

B. Ethical Considerations When Sending Confidential Information Via E-Mail

Attorneys have an ethical obligation to maintain the confidences of their client and communication via e-mail may put those confidences at risk and put the attorney at risk of committing an ethical violation. Rule 1.6 of the Rules of Professional Conduct states in relevant part:

Confidentiality of Information

1. A lawyer shall not reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, . . .

In the Comment to the Rule, it states that a fundamental principle in the client-lawyer relationship is that the lawyer maintain the confidences of the client so that the client will communicate fully and frankly with the lawyer on all subject matters. Rule 4-101 of the Code of Professional Responsibility has similar confidentiality requirements. Modern methods of communication between attorneys and clients and attorneys and third parties raise serious ethical considerations about protecting the client's confidences.

For example, in North Carolina State Bar Op. 215, 1995 WL 853887 (July 21, 1995), the North Carolina State Bar found that "e-mail is susceptible to interception by anyone who has access to the computer network to which a lawyer 'logs on' and such communications are rarely protected from

Because of the lack of security for messages sent on the Internet, the use of e-mail raises questions about whether an attorney or a client can waive the attorney client privilege by sending information via e-mail.

interception by anything more than a simple password." Thus, the North Carolina State Bar concluded that "in using e-mail, or any other technological means of communication that is not secure, an attorney must exercise precautions to protect client confidentiality."

An attorney is not required to use infallibly secure methods of communication, but must implement procedures to effectively minimize the risks that confidential information might be disclosed. That duty includes the obligation to first use reasonable care in selecting a mode of communication that, in light of the exigencies of the existing circumstances will best maintain any confidential information that might be conveyed through that communication. Secondly, an attorney that knows or has reason to believe that the communication over a particular device is susceptible to interception must advise the other party to the communication of the risks of interception and the potential that confidentiality will be lost.

Similarly, the South Carolina Bar Association has ruled that the use of electronic mail to communicate with clients may violate Rule 1.6 of Rules of Professional Conduct absent an express waiver by the client. South Carolina Bar Advisory Opinion 94-27. The Bar Association noted that the very nature of on-line services is such that communications are susceptible to interception and unless confidentiality can be assured when using electronic media, an attorney may run afoul of his/her ethical obligations.

Both the North Carolina State Bar Association and the South Carolina Bar Association relied upon and applied, by analogy, the line of opinions addressing an attorney's ethical obligations with respect to communications by means of cellular or cordless telephones. See Colorado State Bar Ethics Op., 92-90; City of New York Committee on Professional and Judicial Ethics Op. 1994-11 (Oct. 21, 1994); Massachusetts Advisory Op. 94-5; New Hampshire Ethics Op. 1991-92/6 (1992). Because cellular communications are easily intercepted, all of these opinions found that a lawyer who possesses client confidences or secrets must take reasonable steps to secure the information against misappropriation or disclosure. Lawyers should take measures sufficient to ensure within a reasonable degree of certainty that the communications they are engaged in are no more susceptible to interception than a standard land-line telephone call. In addition, lawyers should be very cognizant that even if their own telephones are secure, their clients or other third parties with whom they are speaking may not be secure.

The policy should specify that the e-mail system is the property of the employer and is subject to monitoring at any time, with or without notice, at management's sole discretion.

Because there are methods of scrambling or encrypting signals to prevent interception of cellular and cordless telephone conversations or to reduce the risk of interception, lawyers have an obligation to investigate those methods to satisfy their ethical duties. See Illinois Ethics Op. 90-7; Iowa Ethics Op. 90-44 (1991); Massachusetts Ethics Op. 94-5; New Hampshire Ethics Op. 1991-92/6 (1992). Similarly, there are methods of encrypting e-mail messages and attorneys should research those methods before transmitting confidential information by e-mail.(39)

Another ethics board has reached a similar conclusion with respect to e-mail communications between attorneys and clients. Iowa Ethics Formal Op. 96-1. The Iowa ethics board found that attorneys should not use e-mail to communicate with clients unless they use security measures to protect the confidentiality of information including, encryption or protected password/firewall or first obtain acknowledgment from the client about the risks involved in using e-mail or the Internet.(40)

On March 10, 1999, in Formal Opinion 99-413, the ABA Standing Committee on Ethics and Professional Responsibility joined the clear majority of jurisdictions in concluding that a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct. The ABA Committee found that this mode of transmission affords a reasonable expectation of privacy from both a technological and legal standpoint. The opinion noted that the same privacy accorded United States and commercial mail, land line telephone transmissions, and facsimiles also applies to Internet e-mail. Like other ethics opinions issued on the subject to date, the opinion states that a lawyer should consult with the client and follow the client's instructions as to the mode of transmitting highly sensitive information relating to the client's representation.(41) Given the extent to which state bar associations have looked to the ABA opinions for guidance in the past, it is likely that more states will begin to adopt the analysis found in this new opinion. On April 9, 1999, the Ohio Supreme Court Board of Commissioners on Grievances and Discipline issued a similar opinion, No. 99-2. The board concluded that under normal circumstances a lawyer does not violate the duty under Ohio DR 4-101 to preserve client confidences and secrets by communicating with clients

through unencrypted e-mail. Like the ABA and most of the other state opinions, the Ohio board noted that in matters of extraordinary sensitivity, the lawyer should use heightened security measures appropriate to the situation.(42)

The Third Circuit previously applied similar reasoning in the context of cellular phone communications. In *Shubert v. Metrophone*, Inc., 898 F.2d 401 (3d Cir. 1990), two subscribers of Metrophone filed a claim under the Electronic Communications Privacy Act, 18 U.S.C. 2511(3)(a) on the grounds that Metrophone had intentionally divulged the plaintiffs' cellular phone communications by using a communication method susceptible to interception (i.e., unencrypted and not scrambled). The court rejected the plaintiffs' argument, finding that merely using a method of communication that is susceptible to interception did not constitute an intentional divulgence of information. 898 F. Supp. at 405-406.

C. Waiver Of Attorney/Client Privilege And Work Product Doctrine By Use Of The Internet And/Or Inadvertent Disclosure Through E-mail

The ease with which employers and their attorneys can communicate has greatly increased as both groups "surf" the Internet and communicate via e-mail. As discussed above, because e-mail systems permit the attachment of documents, lawyers and clients can actually conduct business over the Internet. Because of the lack of security for messages sent on the Internet, the use of e-mail raises questions about whether an attorney or a client can waive the attorney client privilege by sending information via e-mail. In addition, as was discussed above, the ease with which an e-mail message can be misaddressed and sent to hundreds or thousands of third parties creates real concerns about the waiver of attorney-client privilege and work product privilege.(43)

There appear to be two types of approaches to inadvertent disclosures of privileged information. There are courts that employ a "bright line" test and there are courts that apply a "balancing test."

Some courts applying a bright line test have concluded that the mere inadvertent disclosure of privileged information does not constitute a waiver of the privilege. See, e.g., *Southeast Banking Corp.* v. FDIC, 212 B.R. 386 (S.D.Fla. 1997) (FDIC's inadvertent disclosure of post-closing documents to bankruptcy trustee did not result in waiver of attorney-client privilege.); T*rilogyCommunications, Inc. v. Excom Realty, Inc.*, 652 A.2d 1273 (N.J.App.Div. 1994) (privileged document disclosed in discovery by attorney did not constitute a waiver of client's privilege); *Georgetown Manor, Inc. v. Ethan Allen*, Inc., 753 F. Supp. 936 (S.D. Fla. 1991) (inadvertent production is the antithesis of concept of waiver); H*elman v. Murray Steaks,* Inc., 728 F. Supp. 1099 (D.Del. 1990); In re Sealed Case, 120 F.R.D. 66 (N.D. Ill. 1988). Other courts applying a bright line test have concluded that any disclosure of privileged material constitutes a waiver of the privilege. See, e.g., *Draus, M.D. v. Healthtrust,* Inc., 172 F.R.D. 384 (S.D.Ind. 1997); *International Digital Systems Corp. v. Digital Equipment Corp.*, 120 F.R.D. 445 (D. Mass. 1988); *Underwater Storage, Inc. v. United States Rubber Co.*, 314 F. Supp. 546 (D.D.C. 1970).

The majority of courts apply some kind of balancing test to determine whether there has been a waiver by inadvertent disclosure of information. See e.g., *McGreevy v. CSS Industries, Inc.*, 1996 WL 412813 (E.D. Pa. 1996); *FDIC v. Marine Midland Realty Credit Corp.*, 138 F.R.D. 479 (E.D. Va. 1991); *Advanced Medical, Inc. v. Arden Medical Servs., Inc.*, 1988 WL 76128 (E.D. Pa. July 18, 1988); *Hartman v. El Paso Natural Gas Co.*, 107 N.M. 679, 763 P.2d 1144 (1988); *Lois Sportswear U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103 (S.D.N.Y. 1985), aff'd, 799 F.2d 867 (2d Cir. 1986). Generally, these cases apply five factors when determining whether an inadvertent disclosure constitutes a waiver:

1. The reasonableness of the precautions to prevent inadvertent disclosure;
2. The time taken to rectify the error;
3. The scope of the discovery;
4. The extent of the disclosure; and
5. The overreaching issue of fairness and justice to the parties.

This analysis applies equally to the work product doctrine. See e.g., *Gold Standard, Inc. v. American Barrick Resources Corp.*, 805 P.2d 164 (Sup. Ct. Utah 1990); *Hartford Fire Ins. Co. v. Garvey,* 109 F.R.D. 323 (N.D. Cal. 1985). Of course, the factors applied by courts are assessed on a case by case basis and the same basic analysis should apply to a disclosure by e-mail or by some other form of communication.

Two unpublished court decisions have found that once information has been published on the Internet, it is no longer protected by the attorney-client privilege or the work product doctrine, regardless of how the information was obtained.(44) The fact that the information had been stolen did not change the fact that the information was in the public domain.

Similarly, in *Castano v. The American Tobacco Co.*, 896 F. Supp. 590 (E.D. La. 1995), the court rejected a claim by Brown and Williamson to protect documents that had been anonymously sent to the University of California library and were published on the Internet. The court found that the documents were in the public domain and, therefore, they could no longer be privileged. Id. at 595-96.

EFFECTIVE AND PROPER E-MAIL POLICY FOR COMPANIES

In order to reduce the potential of liability based on invasion of privacy claims, employers should create and implement a clear e-mail and/or

Internet policy to reduce employees' expectations of privacy. In addition, a clear e-mail policy will define the boundaries of employee conduct with respect to e-mail and the Internet.(45) Policies should differ depending on the business needs of the company, the reasonable expectations of its employees and a balancing of other interests — in other words, an employer must tailor its policy to its unique needs. No matter what the content of the policy is, however, the policy should be given to all employees and placed in the employee manuals. The policy should specify that the e-mail system is the property of the employer and is subject to monitoring at any time, with or without notice, at management's sole discretion.

The following elements should also be contained within the policy, subject to the company's specific needs:

1. The policy should notify employees that the systems are primarily for business use and that the company reserves the absolute right to review, audit and disclose all matters sent over the system or placed into its storage. In addition to the written notification in the handbook or other written materials, ongoing notice to employees can be provided by programming a message that would appear on the employee's monitor each time the employee accesses the system. The policy should also specify that the employer reserves the right to access any messages or information entered into the system.
2. The policy should specify that the system should not be used to communicate any improper communications, e.g., messages which are derogatory, defamatory, obscene or, inappropriate.
3. In order to reduce any reasonable expectation of privacy, the policy should not limit the employer's reasons for monitoring the system as any such limitation could be argued to restrict the scope of the employee's consent to the monitoring. Make clear to employees that using private passwords/codes or making e-mail confidential/private will not limit the employer's ability to monitor its system. A more cautious, but more limiting, approach would be to establish a business purpose that would be articulated in connection with any monitoring so as to defeat any possible expectation of privacy.
4. Consistent with the limitation on non-business use of the system, the policy should be subject to the employer's no-solicitation rule as should all other means of intra-company communication. Such a rule would encompass any solicitation, whether for charitable, personal, business or union organizing purposes.
5. In order to further diminish the reasonable expectation of privacy, the policy should contain a warning that the mere deletion of a message or file may not fully eliminate the message from the system.
6. As further protection, the employer could include a form which employees should be required to sign acknowledging that they have read the policy and acknowledging the employer's absolute right to access the system's information. This could also be accomplished by notice upon login. These will further minimize any expectation of privacy in the information transmitted and should prevent an employee from claiming that he/she was unaware of the policy.
7. The policy should make clear that a violation of the policy may result in disciplinary action up to and including discharge from employment.
8. Monitoring of electronic communications should be limited to situations where such monitoring is necessary to protect the employer's business purposes. The least intrusive method of monitoring the communications should be utilized and excessive intrusion into personal communications should be avoided.
9. In order to reduce the potential for defamation and/or invasion of privacy claims, disclosure of the information obtained from the system should be limited to those who have a legitimate need to know.

Mark S. Dichter is chair of the Labor and Employment Law Practice of Morgan, Lewis & Bockius LLP, a U.S.-based firm which consists of over 180 attorneys in eight offices (www.morganlewis.com). He can be reached at mdichter@morganlewis.com.

Michael Burkhardt is a member of Morgan, Lewis & Bockius' Labor and Employment Law Practice Group in Philadelphia. He can be reached at mburkhardt@morganlewis.com.

Notes

1. Norman, J., "Firm-to-Firm E-Buying Web's Biggest Business," *The Arizona Republic*, Mar. 24, 1999.

2. Hawkins, D., "Office Politics in the Electronic Age Workplace," *U.S.News & World Report,* Mar. 22, 1999.

3. "300 Million Online by 2005 Asia, South America to Lead Way," http://cyberatlas.internet.com/big_picture/demographics/data.html (March 31, 1999)

4. Thomas v. Network Solutions, Inc., 1999 WL 300619, *1 (D.C.Cir.).

5. Nicholson, L., "Oops, Wrong E-Mail Address List. A Dirty Joke Goes Global." *Philadelphia Inquirer,* May 8, 1999.

6. Morgan, Lewis & Bockius' home page on the Web can be found at http://www.morganlewis.com.

7. http://www.nua.ie/survey, Mar. 24, 1999

8. "Over 24 Percent of Employees' Time is Non-Work Related," *Business Wire,* Aug. 11, 1998.

9. Brown., J., "The Mess Made for

Business by Junk Mail," *Business Week*, Apr. 19, 1999.

10. "Over 24 Percent of Employee Time Is Non-Work Related," *Business Week,* Aug. 11, 1998.

11. Jackson, W.,"Survey:Legal Liability of Web Access a Top Concern," *Government Computer News,* Jan. 11, 1999.

12. Carleton, G., "Somebody's Watching, Worker Beware, As Companies Crack Down On E-Mail Abuses," *The Capital Times,* Apr. 9, 1999.

13. Id.

14. "American Management Association: 27 Percent of U.S. Companies Monitor E-mail," http://www.nua.ie/surveys, Apr 16, 1999.

15. Id.

16. Kokmen, L., "Firms E-mull Computer Policies, Employees' Personal Use a Concern," *Denver Post,* Mar. 22, 1999.

17. Ballon, I., The Emerging Law of the Internet, 507 PLI/Pat 1163 (Feb. 1998) (quoting Bohach).

18. Michael Traynor, "Computer E-mail Privacy Issues Unresolved", Nat'l. L.J., (Jan. 1994), at S2 (quoting Bourke).

19. See Natt Gantt, II, L., An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace, 8 *Harvard Law Journal of Law and Technology* 345, at 378-79 (Spring 1995).

20. Id.

21. Id.

22. See Natt Gantt, II, L., An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace, 8 *Harvard Law Journal of Law and Technology* 345, at 398-399 (Spring 1995).

23. Brian D. Pedrow and Debra E. Kohn, "Tampering with E-mail: Proprietary Rights and Privacy Issues", *Law Practice Management,* Nov./Dec. 1995, at 39.

24. Girard, K., "Hold that thought, IS tells e-mailers," *Computerworld,* April 21, 1997.

25. Wright, E., "Executive Secrets: Incriminating Data," *Hemispheres,* June 1993, at 32.

26. McNeil, H. & Kort, R., "Discovery of E-Mail: Electronic Mail and Other Computer Information Should Not be Overlooked," *The Oregon State Bar Bulletin,* December, 1995.

27. Soden, A., "Protect Your Corporation From E-Mail Litigation," *Corporate Legal Times*, May 1995, at 19.

28. Dow Jones Newswires, "International: Microsoft Plied Intuit in 1997, Executive Says," *The Asian Wallstreet Journal*, February 9, 1999.

29. The Supreme Court decision in Zicherman v. Korean Airlines Co., 516 U.S. 217 (1996), later impliedly overruled the portion of the Second Circuit's Lockerbie opinion that suggested that the applicable United States domestic law for determining damages in disasters governed by the Warsaw Convention might be federal common law. However, the Zicherman decision left the damage awards intact.

30. See Reuben, R., Shadow World Searching Information Highway's Sideroads for Evidence, A.B.A. J. 115 (Apr. 1994).

31. See Risk Managing the E-Mail Exposure, Managing Risk LRP Publications (1996).

32. Eric D. Randall, "Internet Pornography and Harassment: Trout v. City of Akron, Ohio Court of Common Pleas, No. 97-115879, December 15, 1998," 1999 No.2 Discrimination L. Update 7.

33. Communications Decency Act of 1996, 47 U.S.C. 230 (Supp. 1996).

34. Zeran v. America Online, 129 F.3d 327, 331 (4th Cir.1997)

35. Allison, G., The Lawyer's Guide to the Internet (1995) at p. 130-131.

36. Mathiason, G. & Juarez, R., "The Electronic Workplace: An Overview," CEB Calif. Bus. L.R., 188,189 (1995) (quoting Borland Int'l, Inc. v. Gordon Eubanks, (Santa Cruz Superior Court No. 123059).

37. Vitoria Slind-Flor, "Silicon Valley is a Big Battleground," Nat'l. L. J., March 22, 1993, at 34.

38. People v. Eubanks, 38 Cal. App. 4th 114, 44 Cal. Rptr. 2d 846 (1995) vacated, 96 C.D.O.S. 9329 (Cal. Dec. 23, 1996)

39. Perritt, Jr., H, Law and The Information Superhighway (1996) at pp. 137-139, 462 (to avoid liability, attorneys must take all reasonable steps to ensure a client's confidentiality including developing security procedures for e-mail communications and using encryption software); Allison, G., The Lawyer's Guide to the Internet (1995) at pp.129-33.

40. A firewall is a method of security that serves as a buffer between the worldwide Internet and secure internal networks. Perritt, Jr., H., What Lawyers Need To Know About The Internet: Basics For The Busy Professional (1996) at 19. A firewall uses one or more computers to prevent outsiders from establishing connections to an internal server. The firewall routes all outside "traffic" to a proxy server that can then distribute the "traffic" to an internal server. Id.

41. *ALAS Loss Prevention Hotline Bulletin No.* 99-9-May 11, 1999.

42. Id.

43. Of course, the concern about misaddressing an e-mail communication is no different that sending a fax to the wrong number.

44. "Tobacco Papers Stay Open," *The National Law Journal*, June 5, 1995 (San Francisco Superior court judge denies claim of privilege for documents that were allegedly stolen and pub-

lished over the Internet); "Mississippi Court Rules Brown & Williamson Documents Not Privileged," West's Legal News, Feb. 9, 1996 (Mississippi state court denies claim of privilege for documents that had been published on the Internet, despite the fact that the documents were allegedly stolen).

45. At least one employer has attempted to use an employee's violation as a legitimate nondiscriminatory reason for an employee's termination. See Lohmann v. Towers Perrin, Forster & Crosby, Inc., 1992 WL 548195 (S.D. Tex. 1992). The employer in Lohmann sought to amend its answer to the compliant to introduce after acquired evidence of employee misconduct relating to unauthorized access to the employer's e-mail system and unauthorized disclosure of information. Although the court did permit the amendment, because Texas law does not recognize the after acquired evidence rule, the facts of the case provide incentive for employers to have a clear e-mail policy that could support a discharge if violated.