

MARGOLIS  
EDELSTEIN

## CYBER-SLEUTH: MONITORING EMPLOYEE E-MAIL

CHRISTOPHER A. TINARI, ESQUIRE

HARRISBURG OFFICE  
P.O. Box 932  
HARRISBURG, PA 17106-0932  
717-975-8114

PITTSBURGH OFFICE  
310 GRANT STREET  
THE GRANT BUILDING  
SUITE 1500  
PITTSBURGH, PA 15219-2203  
412-281-4256

SCRANTON OFFICE  
THE OPPENHEIM BUILDING  
409 LACKAWANNA AVENUE  
SUITE 3C  
SCRANTON, PA 18503  
570-342-4231

MARGOLIS EDELSTEIN  
CHRISTOPHER A. TINARI, ESQUIRE  
THE CURTIS CENTER, 4TH FLOOR  
INDEPENDENCE SQUARE WEST  
PHILADELPHIA, PA 19106-3304  
(215)922-1100  
FAX (215)922-1772  
CTINARI@MARGOLISEDELSTEIN.COM

CENTRAL PA OFFICE  
P.O. Box 628  
HOLLIDAYSBURG, PA 16648  
814-224-2119

WESTMONT OFFICE  
P.O. Box 2222  
216 HADDON AVENUE  
WESTMONT, NJ 08108-2886  
856-858-7200

BERKELEY HEIGHTS OFFICE  
300 CONNELL DRIVE  
SUITE 6200  
BERKELEY HEIGHTS, NJ 07922  
908-790-1401

WILMINGTON OFFICE  
1509 GILPIN AVENUE  
WILMINGTON, DE 19806  
302-777-4680

# **Cyber-Sleuth:**

## **Monitoring Employee E-mail**

Prepared and Presented by:

**Christopher A. Tinari, Esquire**

Margolis Edelstein

Curtis Center, Fourth Floor  
Independence Square West

601 Walnut Street

Philadelphia, PA 19106

215.931.5895 (Voice)

215.922.1772 (Fax)

[ctinari@margolisedelstein.com](mailto:ctinari@margolisedelstein.com)

Visit us at [www.margolisedelstein.com](http://www.margolisedelstein.com)

## Cyber-Sleuth – Monitoring Employee E-mail

Christopher A. Tinari, Esquire

### **I. INTRODUCTION**

E-mail is a highly common, frequent, and ever increasing form of electronic communication both inside and outside the workplace. E-mail can be used as an extremely easy and efficient tool for businesses. However, with e-mail's benefits also come pitfalls. Employees' use of email can cause multiple problems for an employer, even resulting in costly litigation, which is often times grounded in state common law claims against employers as a result of e-mail messages that have been sent in the workplace.

### **II. ISSUES ARISING FROM THE USE OF E-MAIL – WHY EMPLOYERS SHOULD BE CONCERNED**

Examples of problems for and claims against employers from employees' use of email include, but are not limited to, the following:

- A. Decreased business productivity and employee inefficiency (e.g., from overuse or use for personal or non-business purposes)
- B. Quick dissemination and snowballing of office rumors (see Defamation)
- C. Instant distribution of confidential and proprietary company or employee information (trademark, unfair competition, trade

secrets, etc.)

Protection of confidential business information is challenging for all employers. Confidential information is quickly and easily distributed via e-mail. It is documented that employees have used e-mail to transfer files, reports, documents, and other information from their employer to themselves or even to another organization altogether.

1. In New South Communication Corp. v. Universal Telephone Co., 2002 WL 31246558 (E.D. La. Oct. 4, 2002), the plaintiff obtained an injunction after convincing a district court that its former employees had misappropriated trade secret information via the company's e-mail system. An employee who had signed a non-compete agreement with the plaintiff had given his termination notice. He then e-mailed the company's Statement of Income Operations and its report on customer collections to his home e-mail account. The day after he terminated employment, he was able to log onto the company's computer system through his home computer and he proceeded to e-mail himself other documents containing proprietary information and financial information. The Court found that the purpose of the e-mails was to misappropriate confidential and trade secret information.

2. In Equus Computer Systems Inc. v. Northern Computer

Systems, Inc., 2002 WL 1634334 (D. Minn. Jul. 22, 2002), an employee was enjoined from using information he had improperly obtained in competition against his former employer. The employee in Equus had e-mailed a list containing the former employer's customer's buying histories to a competitor. The court noted that by agreeing to the e-mail policy, the employee had agreed to follow company procedures regarding trade secret and confidential information. Likewise, the court found it likely that the former employer would be able to prove that at least some of the material was protectable.

- D. Instant distribution of confidential employee information (this potential problem of e-mail use can lead to other issues, e.g., claims for negligence or invasion of privacy)
  - E. Distribution of improper or obscene material using company resources (this aspect of e-mail use can lead to other issues, e.g., harassment or the creation of a hostile work environment)
  - F. Informality and haste in communication (this aspect of e-mail can lead to other issues, e.g., harassment or the creation of a hostile work environment)
  - G. Harassment and the Creation of a hostile work environment
- See, e.g., Rudas v. Nationwide Mutual Ins. Co., 1997 U.S. Dist. LEXIS

14988 (E.D. Pa. 1997), where the employer was liable for e-harassment of employee by co-worker. Often, the most highly publicized legal exposure associated with e-mail use is employee misuse of e-mail for purposes of harassment. In the context of a hostile work environment/harassment claim, e-mail is simply a new vehicle for an age-long problem.

1. A “hostile work environment” is defined as one that is “so severe or pervasive as to alter the conditions of [the victim’s] employment and create an abusive working environment.” See, e.g., Faragher v. City of Boca Raton, 524 U.S. 775, 768 (1998); see also Meritor Savs. Bank v. Vinson, 477 U.S. 57, 67 (1986). E-mail’s omnipresence, informal nature, illusory privateness, and ease of distribution can contribute to, or even create, a hostile work environment. Employees who are uncomfortable seeing pornographic material or inappropriate jokes in the workplace can claim that they have been subjected to a hostile work environment. In fact, even employees who are uncomfortable knowing that such material is being viewed by co-workers may be able to claim that they have been subjected to a hostile work environment. There is case law in which various courts have affirmed verdicts against employers. In addition, numerous courts have denied employers’ summary judgment motions on hostile environment/harassment claims, sometimes based on the court’s

determination that the e-mails may have at least contributed to the alleged hostile work environment. For example:

2. In Knox v. Indiana, 93 F.3d 1327 (7<sup>th</sup> Cir. 1996), a split jury verdict was affirmed by the court of appeals involving a claim by a New York correctional officer that she had been sexually harassed by her supervisor. Her sexual harassment claim was based in part upon a number of e-mails from the supervisor asking her for sex. The evidence showed that plaintiff made an appropriate complaint to defendant about her supervisor's persistent obnoxious, sexually harassing behavior. The evidence also showed that her complaint was followed by harassment and vicious gossip from her fellow workers, and that the complaint was the cause of the retaliation. Even though a verdict was not returned in favor of the plaintiff on her sexual harassment claim (on the grounds that the employer had taken prompt remedial action when it learned of the e-mails), the jury still awarded \$40,000 to the plaintiff in compensatory damages for the retaliation claim.

3. In Strauss v. Microsoft, 814 F.Supp. 1186 (S.D.N.Y. 1993), the court held that the plaintiff pointed to a number of e-mails that were either sexually explicit or contained sexual innuendo, which showed that the employer's legitimate nondiscriminatory reason

for refusing to promote her was merely a pretext.

4. The plaintiff in Yamaguchi v. U.S. Department of Air Force, 109 F.3d 1475 (9<sup>th</sup> Cir. 1997), relied upon unwanted and inappropriate e-mail messages sent to her from her supervisor to support her sexual harassment claim.

H. Illusion that e-mails are temporary and can be “deleted” (quite often a permanent record of even “deleted” e-mails remains on employers’ computer systems, which often becomes the key evidence in litigation)

I. Intentional infliction of emotional distress

J. Negligent infliction of emotional distress

K. Negligence (e.g., failing to monitor)

L. Intentional interference with contractual relations

M. Invasion of privacy

N. Unfair Labor Practices

1. Section 7 of the National Labor Relations Act, 29

U.S.C. § 157, protects employee activities of an organizational nature. The National Labor Relations Board (NLRB) has attempted to determine just how it is that e-mail fits into the traditional classification scheme that is applied to organizing activities. E-mail has been characterized as a form of

“solicitation,” although it has also been suggested that e-mail deserves its own classification.

2. The NLRB has held that where an employer allows its employees to use the employer’s e-mail system for personal purposes, it is an unfair labor practice for the employer to prevent employees of the bargaining unit from using the e-mail system to distribute union information. See E.I. DuPont de Nemours & Co., 311 N.L.R.B. 893 (NLRB 1993) (approving a finding of violation of Section 8(a)(1) of the Act where employer permitted employees to send e-mail messages on topics including boredom, drugs, and philosophy, but prohibited use to distribute union literature or notices). An employer’s termination of an employee for sending out an e-mail explaining why a modification by the employer of the employee vacation policy was unfair to the employees was deemed to have amounted to concerted activity that is protected by Section 7 of the Act. Timekeeping Systems, Inc., 323 NLRB 244 (1997).

3. The NLRB has attempted to apply labor law to e-mails. In the case of Pratt & Whitney, 1998 WL 1112978 (Feb. 23, 1998), the NLRB’s General Counsel issued an Advice Memorandum in connection with a case that involved several employees who had been disciplined for violations of the employer’s e-mail policy

involving their circulation of union-related information and web postings. The employer's policy prohibited non-business e-mail, but the employer had not been careful in its enforcement of the policy. The question before the NLRB dealt with the validity of the employer's e-mail policy with restrictions. The Advice Memorandum stated that the employer's policy was overly broad and unlawful on its face because it proscribed employee conduct that was protected as "solicitation" under Section 7 of the Act. The NLRB also determined that an employer's restrictive policy was facially unlawful because it did not distinguish between use during "working time" as opposed to "non-working time." TU Electric, 1999 WL 3322181 (Oct. 18, 1999); but see Nat'l Tech Team, No. 16-CA-20176, 2000 WL 1741874 (Apr. 11, 2000) (where the NLRB's General Counsel found that the employer did not violate Section 7 of the Act when it disciplined an employee for generating a piece of pro-union literature on the employer's computer and printer because the employee's misuse of computer resources to create documents during time the employee should have been working is not protected).

### **III. LEGAL CONSIDERATIONS AND PRIVACY ISSUES IN MONITORING**

## **EMPLOYEES' EMAIL**

Employers faced with the myriad of potential problems caused by employees' use of e-mail at the workplace may believe that simply monitoring employees' e-mails, however the employer see fit, is sufficient and adequate protection. However, such monitoring is wholly inadequate and may even lead to additional legal concerns for the employer.

### **A. Employee Privacy Issues**

#### **1. Theft of confidential employee information**

a. The Federal Trade Commission has estimated that 90% of business record thefts involve payroll or employment records.

Identity Theft: Limiting Your Employees' Risk -- And Your Liability, Peter Marshall, <http://hr.blr.com/display.cfm?id=17714> (01/19/2006).

b. A new federal rule (part of the Fair and Accurate Credit Transactions Act of 2003) took effect in June 2005, which requires all businesses (regardless of size) that use a "consumer report" (including background checks done by outside agencies) for business purposes, to properly dispose of sensitive information derived from such "consumer reports". See 15 USCS § 6821 et seq.

c. States are also taking steps to protect sensitive information.

For example, Georgia passed a law requiring employers to destroy certain documents, while a law became effective in California on July 1, 2005 that restricts public display of social security numbers on employee badges and documents. In Michigan, employers were required to do the same as in the California law beginning January 2006. Use of social security numbers is also now restricted in Arizona, Arkansas, Missouri, Texas, and Virginia.

d. New Jersey passed the Identity Theft Protection Act, P.L. 2005, c 226, which became effective January 1, 2006. The Act creates liability for failing to safeguard personal data such as social security numbers, drivers' license numbers, state ID card numbers, credit or debit card numbers, or any other number which would provide access to a person's finances. It creates an individual cause of action against violators and even permits treble damages and attorneys' fees for willful or negligent violations. Elements of the NJ Act include the following:

- i. any business that compiles social security numbers must promptly disclose breach of security in writing; disclosure may be done on website if cost of disclosure exceeds \$250,000;
- ii. breaches of security must be reported to the state

police and local police departments must take reports from victims of identity theft;

iii. employers must take “reasonable” measures to dispose of records in a way that would prevent interception (e.g., destroying electronic media);

iv. employers who conduct credit or background checks on job applicants must provide applicants who are rejected on the basis of discovered information a summary of rights.

e. If an employer is keeping personnel records in an electronic format, such location on the employer’s network should be secure so that no one else (even including members of the company’s technology department) can access it.

f. If an employer is keeping medical information in electronic format, it should be kept in a secure domain accessible only to those responsible for administering the data. Employers should take steps to ensure that members of the technology department do not have access to the information.

2. Employees’ false expectation of privacy

a. See Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996), in which an at-will employee claimed that he had been

unlawfully discharged for sending inappropriate and unprofessional e-mails. The employee alleged that his termination violated Pennsylvania's public policy against the invasion of privacy. The court determined that the employer's interception of plaintiff's inappropriate e-mail communications over the company e-mail system did not tortiously invade plaintiff's privacy and, thus, did not violate public policy. After defining the narrow parameters of the claim, the court found that the employee had no reasonable expectation of privacy in his email once he voluntarily sent an email to a second person over the company's e-mail system.

The Smyth court distinguished that type of situation from the situation where an employer mandates a drug test or conducts a search of personal property, reasoning that where the employee's conduct was voluntary, the employer's conduct could not be considered a highly offensive invasion of privacy.

b. See Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 107 (3d Cir. 2003), in which the Third Circuit held that an insurance company acted lawfully in retrieving stored e-mail communications from a computer that was used by one of its insurance agents.

The Third Circuit in Fraser agreed with the employer and

under

“every other circuit court to have considered the matter” that, the federal Electronic Communications Privacy Act (ECPA), an intercept “must occur contemporaneously with transmission,” to be covered by the ECPA. In addition, because the e-mail was stored on the company’s system, the search fell within an exception to the Act, which covered seizures of e-mail that had been authorized “by the person or entity providing a wire or electronic communications service.”

c. The aforementioned rulings notwithstanding, the best practice is for an employer to clearly state that an employee has no expectation of privacy in email (discussed in detail below). See McVeigh v. Cohen et al., 983 F. Supp. 215 (D.C. 1998), in which employee prevailed because his employer (the U.S. Navy) discharged employee because of the contents in “a private anonymous email” sent by McVeigh – which meant the content of the email did not violate the military’s “don’t ask, don’t tell” policy.

## B. Statutory Considerations

### 1. Federal Electronic Communications Privacy Act (“ECPA”)

a. Enacted by Congress in 1986 to amend the Federal Wire Tap Act of 1968, the ECPA prohibits interception of “wire, oral or

electronic” communications, as well as the disclosure and use of such information. 18 U.S.C. § 2511.

b. The purpose of the ECPA is to provide forms of electronic communications with protection against improper interception.

c. Under § 2520, recovery of civil damages is authorized and those who violate the ECPA may be liable for punitive damages, as well as the greater of the following:

- I. actual damages plus profits made by the violator;
- ii. \$100.00 per day for each day of the violation; or
- iii. \$10,000.00

d. There are two exceptions, which permit employers to intercept electronic communications in the workplace context, although these exceptions are limited. The exceptions do not guarantee that an employer who conducts employee monitoring without first communicating a written information control policy will escape liability:

- i. Business extension exception

To intercept a communication under the ECPA is to acquire “the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other devise.” 18 U.S.C. § 2510(4). The business extension

exception excludes from the definition intercepting devices those devices “furnished to the subscriber or user by a provider of wire or electronic communication service” and being used “by the subscriber or user in the ordinary course of its business.” 18 U.S.C. § 2510(5)(a). Thus, if the intercepting equipment is furnished to the employer by a provider of communication services, and if the interception is made in the ordinary course of the employer’s business, there is no “interception” as defined by the Act and, therefore, no violation of the ECPA.

ii. Consent Exception

Interception is also not a violation under the ECPA if “one of the parties to the communication has given prior consent to such interception.” 18 U.S.C. § 2511(2)(d). (But see discussion of the Pennsylvania statute). An important point to be aware of regarding this exception is that employee knowledge of monitoring does not necessarily equal consent to such monitoring. See, e.g., Jandak v. Village of Brookville, 520 F.Supp. 815 (N.D. Ill. 1981). While consent may be implied from the surrounding circumstances indicating that the party knowingly agreed to

the surveillance, the notice of “constructive consent” has been rejected by most courts. See, e.g., Grigg-Ryan v. Smith, 904 F.2d 112 (6<sup>th</sup> Cir. 1990); Jandak v. Village of Brookville, 520 F.Supp. 815 (N.D. Ill. 1981). It has, however, been approved by at least one court. Griffin v. Milwaukee, 74 F.3d 824 (7<sup>th</sup> Cir. 1996).

2. PA and NJ Electronic Surveillance Statutes

a. Pennsylvania Wire Tapping and Electronic Surveillance Act, 18 PA. C.S.A. § 5701, et al.

Provides “business extension” and “consent” exceptions to liability, but requires that all parties to the communication must have given prior consent to the interception, while the federal ECPA requires the consent of only one party. Maryland has a similar statute.

b. New Jersey Wiretapping and Electronic Surveillance Control Act (NJSA 2A:156A-1, et al.)

Substantially resembles the federal statute, including requiring the consent of only one party. Interestingly, the Act does not apply to e-mail received by the recipient, placed in post-transmission storage, and then accessed by another without authorization.

Under the Act, accessing someone's e-mail "without authorization" in violation of 2A:156A-27(a) means using a computer from which one has been prohibited, or using another's password or code without permission. Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F.Supp.2d 817 (E.D. Mich. 2000). Where a party "consents to another's access to its computer network, it cannot claim that such access was unauthorized." Id. at 821.

Under the Act, an "electronic communication," by definition, cannot be "intercepted" when it is in "electronic storage," because only "communications" can be "intercepted," and ... the "electronic storage" of an "electronic communication" is by definition not part of the communication. See Bohach v. City of Reno, 932 F.Supp. 1232, 1236 (D. Nev. 1996). The treatment of messages in "electronic storage" is not governed by the restrictions on interception. "Intercept" does not apply to "electronic storage." See Steve Jackson Games Inc. v. United States Secret Service, 36 F.3d 457, 462 (5th Cir. 1994).

3. Computer Fraud and Abuse Act (18 U.S.C. § 1030)
  - a. Provides companies with a cause of action against those persons who "knowingly cause the transmission of a program,

information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.” 18 U.S.C. § 1030(a)(5)(A)(I).

The term “protected computer” means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States. 18 USCS § 1030.

b. The Computer Fraud and Abuse Act may also offer employers protection against disgruntled employees, as well as outsiders. See International Airport Centers, LLC et al., v. Jacob Citrin, No. 05-1522 (7<sup>th</sup> Cir., March 8, 2006).

C. Duty to Monitor

1. For the most part, case law has dealt with the *right* of employers to

monitor employee activity. However, in a recent New Jersey Appellate Division case, Doe v. XYZ Corp., 382 N.J. Super. 122 (App. Div. 2005), a three-judge panel actually imposed a *duty* on the employer to thoroughly investigate and take prompt remedial action to stop an employee's improper use of a company computer. With this decision – the first of its kind in the country – employers are faced with important new burdens.

In Doe, Plaintiff, a mother, individually and on behalf of her minor daughter, appealed the order of the Superior Court of New Jersey, Law Division, Somerset County (New Jersey), which granted summary judgment to defendant corporation. The mother brought a negligence suit, alleging that the corporation breached a duty with regard to allowing an employee to use, view, and download child pornography on its computer at his workstation without reporting him.

The employee was the mother's husband and worked for the corporation as an accountant. It was discovered that he was secretly videotaping the mother's 10-year-old daughter at their home and sending the photos to child pornography sites using the corporation's computer at his workstation. His computer showed e-mails being sent to pornographic websites and interactions with others regarding child pornography.

The corporation had become aware of the employee viewing pornography, including child pornography, but did not do much to

stop the employee other than to confront him on occasion. Eventually, the employee was arrested on child pornography charges. The corporation knew that the employee had a wife and child since, among other things, they had attended company outings with him.

In granting summary judgment, the trial court determined that the corporation had no duty to investigate the private communications of the employee and that it had no control over the employee's conduct at home. However, the appellate court disagreed and held that there was no expectation of privacy on the part of the employee and that the corporation was on notice that the employee was viewing pornography on the work computer. As such, the corporation had a duty to report the employee's activities to the proper authorities and to take effective internal action to stop those activities.

#### **IV. HOW TO AVOID EMPLOYEE PRIVACY CLAIMS AND OTHER CLAIMS RELATED TO E-MAIL USE**

The numerous problematic issues and situations that result from employees' use of e-mail continue to demonstrate the important need for employers to have e-mail policies, to educate their employees about those policies, and to consistently enforce those policies.

- A. Create and implement written policy
  - 1. Establish and distribute policy prohibiting improper use of e-mail

and stating that e-mail is monitored – (e.g., MCI Worldcom Inc. avoided liability as a result of effective policy).

2. Clearly and unambiguously state that employees have no expectation of privacy in the use of the employer's communication system.
3. Ensure that employees sign an acknowledgment that they have read and understood the policy.

B. Provide training on the policy

1. Employers should provide training to employees on proper use of e-mail, with an emphasis on the important need for careful and professional communication, as well as sensitivity to issues that would be privileged if not copied to parties (thereby breaching the privilege).
2. Make certain that employees understand that there is no expectation of privacy.
3. Be sure that employees understand that inappropriate use of technology will not be permitted or tolerated by the employer.
4. Make sure that employees understand what exactly constitutes improper use of e-mail under the policy.
5. See Daniels v. Worldcom Corp., 1998 WL 91261 (N.D. Tex., Feb. 23, 1998) (employer successfully defended claim of negligence case arising from improper use of email to distribute racist jokes because it responded promptly to complaint and conducted training session).

See Schwenn v. Anheuser-Busch, Inc., 1998 WL 166845 (N.D. NY April 17, 1998) (employer successfully defended sexual harassment suit because it had a policy expressly prohibiting use of email to send sexually inappropriate communications).

C. Scope and Content of E-mail Policy

The employer's e-mail policy should be as clear as possible to reduce an employee's expectation of privacy, as well as to define the boundaries with respect to employee conduct via e-mail.

1. Policy Examples

a. An employer may choose to completely prohibit the use of e-mail for non-work purposes. Such a policy should be uniformly administered throughout the company.

b. An employer may also choose to prohibit e-mail for non-work purposes during work time, which would allow employees to use e-mail during breaks or after hours. Under such a policy, an employer should include a prohibition against both sending and opening personal e-mail during non-work hours, with definitions for what constitutes "work time" and "personal e-mail."

c. An employer could also choose to allow personal use of e-mail within certain boundaries (e.g., restrict certain websites).

Many businesses might choose this option in the interest of

keeping up employee morale and not wanting to appear overbearing to its employees.

2. Content of Policy

a. Any e-mail policy should inform employee that the e-mail system is the employer's property and is intended principally for business purposes.

b. Any e-mail policy should contain a statement that notifies employees that they do not have an express or implied personal privacy right in any matter created, received, or sent from an e-mail system.

c. Employees should be warned that there are security risks associated with electronic communications.

d. The policy should be accompanied by a form that the employees are required to sign, acknowledging the e-mail policy and the employer's absolute right to monitor e-mail.

e. The policy should also contain a statement that any violation could result in disciplinary action, up to and including termination.

D. Conduct random and even-handed monitoring, as disclosed in the policy – see Wildberger v. Fed. Labor Relations Auth., 132 F.3d 784 (D.C. Cir. 1998) and Cochrane v. Houston Light & Power Co., 996 F. Supp. 657 (S.D. Tex. 1998)

(alleging email policies were applied in a discriminatory manner)

E. Provide for “signing” of electronic communications using digital certificate technology

F. Use encryption technology to “seal” emails by scrambling their content – see *Avoiding Pitfalls in Effective Use of Electronic Mail*, K. Robert Bartram, Pa. Bar Assn. Quarterly (Jan. 1998)

G. In appropriate situations, employers can seek injunctive relief – See, e.g., *Intel Corporation v. Hamidi*, No. 98AS05067 (Cal. Sup. Ct., Nov. 24, 1998), in which the court granted an injunction against a former employee who sent mass email messages to thousands of current Intel employees criticizing the company’s personnel policies, holding that a company’s internal email address system is proprietary and is not meant for use outside the company. The court declared that the former employee had no constitutional right to access the company’s internal email system.

H. Include a disclaimer on e-mails

It is not certain whether or not an email disclaimer protects a company from liability, but it can certainly help a company’s case and in some situations might even exempt a company from liability. A disclaimer may even help to prevent the actual occurrence of lawsuits against a company since just the presence of the disclaimer could potentially deter many people from filing suit. Disclaimers can help protect against breach of confidentiality, transmission of viruses,

inadvertently entering into contracts, negligent misstatement, and liability for the employer. A disclaimer will not protect against defamation, although it could help reduce the company's percentage of liability.