Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 1996 Proceedings

International Conference on Information Systems (ICIS)

December 1996

United States Cases of Employee E-Mail Privacy Intrusions: Do You Really Know the Legal Consequences?

Janice Sipior
Villanova University

Burke Ward
Villanova University

Follow this and additional works at: http://aisel.aisnet.org/icis1996

Recommended Citation
Sipior, Janice and Ward, Burke, "United States Cases of Employee E-Mail Privacy Intrusions: Do You Really Know the Legal Consequences?" (1996). *ICIS 1996 Proceedings*. 16.
http://aisel.aisnet.org/icis1996/16

This material is brought to you by the International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 1996 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

UNITED STATES CASES OF EMPLOYEE E-MAIL PRIVACY INTRUSIONS: DO YOU *REALLY* KNOW THE LEGAL CONSEQUENCES?

Janice C. Sipior
Burke T. Ward
Villanova University

Abstract

Employers and employees are both highly vulnerable to negative consequences which may result from e-mail privacy intrusions. These intrusions may arise internally from co-workers or the employer, or externally from entities associated with the U.S. legal system, such as law enforcement agencies or attorneys, or from hackers. Given potentially differing perceptions regarding e-mail privacy and the problems which may result from privacy intrusions, there is a need to recognize and understand privacy issues associated with e-mail use. In this paper, we first review the U.S. legal system to reveal the surprising lack of e-mail privacy protection currently afforded. Based on this legal review, a framework is presented to identify the potential legal consequences under varying circumstances in the workplace. Finally, example e-mail privacy cases are discussed, within the context of the framework, to illustrate issues associated with e-mail privacy intrusions.

1. INTRODUCTION

A Louis Harris survey revealed 53% of Americans are very concerned about privacy, the first time a majority has held this concern (Harper 1993). Further, many would prefer to interact with a company which protects their privacy. The privacy issues associated with electronic mail (e-mail), an increasingly common form of communication technology, have not yet been well-defined. Indeed, Scott Charney, chief of the computer crimes unit of the Justice Department, recently stated, "The system sprang up so quickly that what constitutes acceptable or unacceptable behavior has never been established. No one knows where they stand" (Ewell 1994). The rapid pace of technological advances creates a challenging environment for both employers and employees alike in addressing privacy. Technological innovation proceeds at a much faster pace than corresponding changes in the law. However, law is often the vehicle for formally implementing guidelines and procedures, in response to societal pressure to enforce ethical conduct. Thus, societal pressure acts as a barometer for the formation of legal parameters.

Users and organizations who are naive about societal pressure for ethical conduct and the legal parameters concerning e-mail privacy are both highly vulnerable to negative consequences which may result from intrusions. In this paper, we first review the U.S. legal system to reveal the surprising lack of e-mail privacy protection currently afforded. Based on this legal review, a framework is presented to identify the potential legal consequences under varying circumstances in the workplace. Finally, example e-mail privacy cases are discussed, within the context of the framework, to illustrate issues associated with e-mail privacy intrusions.

1. EMPLOYEE E-MAIL PRIVACY PROTECTION IN THE U.S. LEGAL SYSTEM

An extensive review of e-mail privacy protection concluded that none of the elements currently within the U.S. legal system seem to offer significant protection for the privacy of employees in their e-mail communications (Sipior and Ward 1995). E-mail monitoring is not specifically addressed in any of the current components of the U.S. legal system. Consequently, issues of e-mail privacy must be assessed through protections established for employee privacy in general. An analysis of these protections as applied to e-mail is reviewed below and summarized in Table 1 to provide the reader with an understanding of the legal elements, including federal and state constitutional law, state common law, federal and state statutes and judicial decisions, under which e-mail privacy cases may be filed.

Table 1. Employee Privacy Protection Within the United States for E-mail Communications

LEGAL PROTECTION	INTERPRETATION FOR E-MAIL
I. Constitutional Protection	
1. U.S. Constitution Fourth Amendment	Generally, only public sector employees of federal, state, and local government have limited privacy protection. To date, there is no precedent for e-mail.
2. State Constitutions	Privacy protections, if any, vary substantially from state to state. California has the most developed state constitutional privacy protection. The effect on e-mail still remains unclear.
II. State Common Law Protection	Continuously developing through state court decisions, e-mail privacy protection, if any, is contained in the tort of invasion of privacy and causes of action related to this tort.
III. Statutory Protection	There has not been much state or federal legislation with respect to e-mail privacy.
1. Federal Statutes	
Electronic Communications Privacy Act (ECPA) of 1986	Exceptions stated in this Congressional Act appear to leave employee e-mail privacy unprotected.
Proposed Privacy for Consumers and Workers Act	Since 1991, this Act has been debated in both houses, the U.S. Senate and the House of Representatives, of the U.S. Congress.
2. State Statutes	Privacy protections, if any, vary from state to state. Regulation is primarily at the federal level through the ECPA. States may, in some instances, enact statutes more stringent than the federal statute.

From: Sipior and Ward 1995.

2.1 U.S. Constitutional Privacy Protection

The U.S. Constitution, in part, defines the relationship between the U.S. government and its citizens. Regarding privacy, the Fourth Amemdment to the U.S. Constitution provides, in part, that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." Although the words "the people" would seem to include all employees, it is usually only public sector employees of federal, state, and local governments who have privacy protection under the Constitution (Griffin 1991). Constitutional protection can be extended to private sector employees only in instances where they can successfully demonstrate sufficient governmental involvement, referred to as "state action" (*Skinner v. Railway Labor Executives Association* 1989).

Public sector employees' privacy protection under the Fourth Amendment is not unlimited. In a precedent-setting employee privacy case, *O'Connor v. Ortega* (1987), the U.S. Supreme Court ruled in favor of the employer, based on (1) whether or not the employee, Ortega, had a reasonable expectation of privacy, and (2) whether or not the employer's search of his office was unreasonable. On the first point, the Court held that since Ortega had a private office, he did have a reasonable expectation of privacy. However, the Court found the search of his office to be reasonable since it was work-related. The government's need to ensure efficient operation of the workplace outweighs an employee's expectation of privacy, even if the privacy

expectation is reasonable. For e-mail communications, the extent of constitutional protection is unclear. E-mail is not like a locked desk or file cabinet. The employer has access to all messages on the system. It could therefore be argued that the public sector employee's legitimate expectations of privacy in e-mail communications are diminished.

2.1 State Constitutional Privacy Protection

Some state constitutions specifically grant individuals an explicit right to privacy (Baumhart 1992; Griffin 1991). Again, this right usually extends to protection for public sector, not private sector, employees. In California however, the state Constitution was amended to include privacy protections. A California appellate court specifically held that the right of privacy applied to both public and private sector interests (*Wilkinson v. Times Mirror Corporation* 1989). Further, the case of *Soroka v. Dayton Hudson Corporation* (1992) reaffirmed this and held that an employer may not invade the privacy of its employees absent a compelling interest. In *Soroka*, the invasive action by the employer was the administration of a psychological screening test to job applicants. Similarly, some compulsory employee drug testing has been held to violate this state's constitutional privacy right (*Luck v. Southern Pacific Transportation Company* 1990). How this may apply to e-mail, if at all, remains to be decided.

2.3 State Common Law Privacy Protection

Common law is a continuously changing system of law, developed and updated by judicial decisions based on precedent and societal values, rather than on written laws (i.e., statutory law). The common law privacy claim most likely to be asserted in response to the monitoring of an employee's e-mail is the tort of invasion of privacy, more specifically, intrusion upon seclusion (Griffin 1991). This theory considers privacy as based broadly on concepts of individual human dignity and respect rather than a separate independent value (*Harvard Law Review* 1991).

To apply the tort of inclusion upon seclusion to e-mail privacy, an employee whose e-mail has been unknowingly monitored must demonstrate (1) an intrusion, (2) into a private affair or concern, and (3) that the intrusion would be highly offensive to a reasonable person (*Restatement (Second) of Torts* 1977). The undisclosed monitoring of e-mail would seem to be an intrusion, but are messages on an employer's e-mail system private since the system is for the employers' business purposes? The answer is unclear, but courts have extended privacy protection to the analogous areas of wiretapping telephone calls and intercepting written communications (Griffin 1991). Regarding the third element, whether e-mail monitoring would be highly offensive to a reasonable person, the same rationale would seem to apply. This monitoring is done on equipment owned by the employer, used ostensibly for the employer's purposes, by a compensated employee. It is arguable that this environment should not give rise to a reasonable expectation of privacy. To date, there is no definitive answer to whether this tort applies to the monitoring of e-mail.

2.3 Federal Statutory Privacy Protection

Constitutional law and common law protections of e-mail privacy are, at best, vague. As part of the heated ethical and political debate over privacy issues, certain specific statutory protections have been enacted and/or proposed by the U.S. Congress. The most important among these for e-mail privacy is the Electronic Communications Privacy Act (ECPA) of 1986, since internal company e-mail systems were not covered by any federal statute prior to this act (Office of Technology Assessment 1985). The ECPA amends existing federal wiretap law to include most electronic communications. Its purpose is to extend existing privacy protections against wiretapping to new forms of electronic communications, such as electronic mail, cellular telephones, and data transmission, from improper interception. Broadly, the ECPA prohibits the interception of wire, oral, or electronic communication, and the disclosure or use of such intercepted communication. The statute's broad definition of electronic communication clearly includes e-mail within its scope. Further, in Title II, the ECPA, subject to significant exceptions, prohibits access and/or disclosure of stored electronic communications.

Two exceptions in the ECPA make it unclear as to whether e-mail monitoring by private sector employers is covered. The first, referred to as the business use or business extension, is a common defense in cases brought under the ECPA (Griffin 1991).

To be an effective defense against an employee's claim of e-mail privacy invasion, the employer must demonstrate that a business use was the reason for the interception and that monitoring was conducted within the ordinary course of business (*Watkins v. L. M. Berry & Company* 1983). In *Watkins*, the employer notified the employee that telephone sales calls were being monitored. This notification was interpreted to mean that the specific interception was in the ordinary course of business. The business purpose ended when it became apparent that the telephone communication was personal. Although this exception has been applied to telephone communication, it would seem to apply equally to e-mail. If an employer wants to ensure that its e-mail system is used solely for work-related purposes, then routine monitoring of the content of e-mail messages might fall under this exception.

The second exception in the ECPA, called the prior consent exception, may actually permit telephone and e-mail monitoring. Under this exception, employers may be able to protect themselves against the risk of liability merely by notifying one of the parties that his e-mail may be examined. Such consent may be express or implied, but is limited to the scope of the consent. In *Watkins*, the consent was only to the monitoring of business calls. The court refused to extend this consent to all telephone calls. A review of relevant legal research seems to conclude that the ECPA does not afford significant privacy protection to employees' e-mail communications (Griffin 1991; *Harvard Law Review* 1991; and Hernandez 1988).

2.5 State Statutory Privacy Protection

Privacy protections of electronic communications vary from state to state, but are primarily regulated at the federal level by the ECPA. Most states have addressed these issues through either wiretapping legislation or electronic monitoring legislation, or both (Griffin 1991). Generally, these state efforts have not been effective in protecting an employee's e-mail privacy.

In 1990, an attempt was made to find employee e-mail privacy protection within California's criminal laws (*Shoars v. Epson America, Inc*. 1990). California Penal Code Section 630 prohibits wiretapping without the consent of all parties involved, and also states that a person may not "read or attempt to read, learn the contents or meaning of any message report, or communication while the same is in transit or passing over any such wire, line or cable, or is being sent from, or received at any place within the state." In January 1991, a Superior California Court Judge dismissed the *Shoars v. Epson America, Inc*. lawsuit, ruling that Section 630 did not apply since the legislation did not specifically refer to e-mail.

3. THE CONSEQUENCES OF EMPLOYEE E-MAIL PRIVACY INTRUSIONS WITHIN THE UNITED STATES

It is evident from the discussion of the U.S. legal system that cases of employee e-mail privacy intrusions may be filed under various legal elements, depending on the circumstances of the particular case. Although each is unique, a factor common to the cases is whether the employee has a legitimate expectation of privacy. This expectation may be heightened or diminished based on factors present in the work environment. A framework depicting the major factors which confront employees in their e-mail communications and the legal consequences, in terms of the employee's expectation of privacy, is presented in Figure 1.

Intrusions may occur within or outside of an organization. Within an organization, a formal e-mail privacy policy may or may not have been established. Further, this policy may either provide employees with assurances that e-mail will remain private, or alternatively, inform employees the company reserves the right to monitor communications. Although there is no count of the number of organizations which currently have an e-mail policy, a recent survey suggests few companies have either formulated a policy or effectively communicated the policy to employees (ZifNet 1993). Of 204 respondents, only 16% indicated that their company has a policy; over 35% were unaware of the existence of a policy. Finally, intrusions from various sources external to an organization are a continuous threat, from both legal agents and illegal perpetrators. To illustrate the consequences for each of the cells depicted in Figure 1, the following sections discuss example cases, which are summarized in Table 2. The cases discussed include only those reported by WestLaw, a major U.S. legal database service, or by the media. Many cases are settled out-of-court and most lower state court decisions generally are not reported.

	INTERNAL ORGANIZATIONAL ENVIRONMENT			EXTERNAL ENVIRONMENT
	Formal E-mail Privacy Policy		No Formal E-Mail Privacy Policy	**Cell 7**: E-mail always subject to intrusions from: • Court discovery process (subpoena) • Law enforcement (search warrant) • Hackers
	E-mail Privacy is Assured	E-mail is Not Private		
Employer Monitors E-mail	**Cell 1:** Potential lawsuit claiming reasonable expectation of privacy, but result depends on state law.	**Cell 3**: Potential lawsuit, case law indicates no reasonable expectation of privacy.	**Cell 5**: Potential lawsuit, arguably a reasonable expectation of privacy based on password access.	
Employer Does Not Monitor E-mail	**Cell 2**: No Legal Consequence.	**Cell 4**: No Legal Consequence.	**Cell 6**: No Legal Consequence	

Figure 1. Framework of Legal Consequences for Employee E-mail Privacy Intrusions

3.1 Assurances of Privacy Communicated via a Formal E-mail Privacy Policy

If a privacy policy, explicitly assuring e-mail to be private within an organization, were formally established and communicated (Cell 1), employees would rightfully have a heightened expectation that e-mail will remain unseen by organizational members, other than the intended recipient(s). The legal consequence for monitoring employee e-mail under these conditions is likely to be a lawsuit against the employer based upon the employee's reasonable expectation of privacy. This expectation seems well-founded since the employee was explicitly assured, through a formal company policy, that e-mail communications are private. However, the outcome is surprisingly not so clear.

The Pillsbury Company in Pennsylvania repeatedly assured employees that all e-mail was confidential, and further that it could not be intercepted and used against them. Relying on this policy, Michael A. Smyth, a regional operations manager, responded to e-mail he received at home from his supervisor. Contrary to the assurances of confidentiality, the e-mail correspondence was intercepted. Smyth was terminated for inappropriate and unprofessional statements in his e-mail messages. In response, Smyth filed a wrongful discharge suit (*Smyth v. The Pillsbury Co.* 1996). Applying the Pennsylvania tort of invasion of privacy, more specifically, intrusion upon seclusion, the court found there was no reasonable expectation of privacy since the e-mail correspondence was voluntary, even though privacy in such communications had been assured. The company's interest in preventing inappropriate or even illegal message content was found to outweigh any privacy the employee may have had, regardless of assurances to the contrary.

Obviously, in the converse instance wherein the employer explicitly states e-mail correspondence will remain private within an organization and abides by its own policy (Cell 2), no legal consequence would result. Nothing would prompt an employee to initiate legal action against the employer.

3.2 Employer's Right to Monitor E-mail Communicated via a Formal E-mail Privacy Policy

A company may inform employees that it reserves the right to monitor e-mail messages (Cell 3). The employer has an interest in effectively managing this resource since he can be held liable for its inappropriate use by employees. Indeed, e-mail and

Table 2. Example Cases of Employee E-mail Privacy Intrusions Classified According to the Framework in Figure 1

	EXAMPLE CASE	ACTION	CONSEQUENCE
Cell 1	*Smyth v. The Pillsbury Co.*	Under assurances of e-mail privacy, employee responds to e-mail from home.	Employee fired for e-mail content.
Cell 3	*Bourke v. Nissan Motor Corporation in USA*	Password protected e-mail is read by supervisor.	Two employees fired for e-mail content
Cell 5	*Shoars v. Epson America Inc.*	E-mail is routinely printed and read.	Employee fired for protesting e-mail monitoring
	Colorado Springs Mayor and City Council	Mayor prints and reads Council members' e-mail, believing messages are covered by the state's broad public-records law.	One Councilman reportedly considered filing criminal charges against the Mayor.
	Borland International, Inc. v. Symantec Corp.	Former employees e-mail is retrieved from company-provided external e-mail system.	Lawsuit is pending.
Cell 7	Senate Whitewater Hearings	Secretaries exchange comments via e-mail.	Public discussion of e-mail content not intended to be shared.
	Intuit, Inc.	Indiscriminate back-up of company records	Justice Dept. Searches through 80,000 e-mail messages.
	Iran-Contra Investigations	Oliver North and John Poindexter delete e-mail, unaware of automatic back-up and capability of retrieval from White House back-up tapes.	Public discussion of e-mail content not intended to be shared.
	Chevron Corporation	Deleted e-mail, retrieved from archives, used as evidence in a sexual harassment case.	Four female employees receive a settlement of $2.2 million.
	Siemens Solar Industries v. Atlantic Richfield Co.	Deleted e-mail, retrieved from archives, used as evidence in a federal securities fraud case.	Siemens' claims were ultimately dismissed as untimely.
	Electronic Evidence Discovery Inc.	Deleted and overwritten e-mail, expertly recovered, used as evidence in sexual harassment case.	A female employee receives a settlement of $250,000.
	Vermont Microsystems Inc. v. Autodesk Inc.	Suspicious e-mail content, coupled with existence of permanent file deletions, used as evidence in a trade secrets allegation.	Vermont Microsystems awarded $25.5 million in damages.
Other	Los Angeles Times	Moscow correspondent accesses co-workers' password controlled e-mail accounts and reads messages.	Correspondent subjected to the disciplinary action of reassignment to an undisclosed position.

other electronic information are considered to be emergent sources of discovery in lawsuits (McNeil and Kort 1995), as will be exemplified through cases presented in the discussion of intrusions from external sources (Cell 7). Other reasons for monitoring e-mail include tracking employee work performance, safeguarding the security of company resources against theft or espionage, resolving technical problems, and containing costs. Even when an employer explicitly communicates its e-mail monitoring practices, employees may still expect their e-mail messages to remain private.

Two employees at Nissan Motor Corporation in Carson, California, Bonita B. Bourke and Rhonda L. Hall, were hired to implement and maintain an internal e-mail system between Nissan and its Infiniti dealerships. The two believed messages to be confidential since the e-mail accounts were password protected. In the process of training dealers, the e-mail correspondence became friendly. A supervisor, who printed and read the messages, threatened to discharge them (Wiegner 1992). Bourke claims to have been forced to resign, Hall was fired (Nash and Harrington 1991). The ensuing case, *Bourke v. Nissan Motor Corporation in U.S.A.*, alleged invasion of privacy and wrongful termination in violation of California statutes (Traynor 1994). The California Intermediate appellate court upheld the judgment in favor of the employer. It also upheld the lower court's consequent rejection of the employees' claims. The employees had no reasonable expectation of privacy because they had signed a user registration form stating that company policy to restrict use of the company's e-mail system to company business and that e-mail was periodically monitored.

Again, in the converse instance wherein the employer does not engage in monitoring activities, it is obvious that no legal consequence would result. Regardless of whether the employer has explicitly stated e-mail will be monitored (Cell 4) or remain private, as long as monitoring is not done nothing would prompt an employee to initiate legal action against the employer.

3.4 No Formal E-mail Privacy Policy

In a legal manual written for systems personnel, it was stated that in the absence of a formal e-mail privacy policy, an employer may implicitly assure e-mail is private by the absence of monitoring. "If an employer knowingly allows private employee electronic mail to grow and flourish on the company system without opposing it, then an implied agreement can be established, under which employees have a right to expect their private transmissions to remain private" (Rose and Wallace 1992, pp. 101-102). Neither case law nor legislation has supported this contention. Nonetheless, employees have acted under the assumption that e-mail is private, even though their employer never formally established that it is.

At Epson America, Inc. in Torrance, California, Alana Shoars, Office Systems Programmer Analyst, was responsible for installation and training for an office e-mail system. In this capacity, she assured employees that e-mail communications were private (Winters 1993). However, her supervisor, Robert Hillseth, the manager of the mainframe that routed messages between the company's internal e-mail system and its external MCI e-mail service, placed a tap on the gateway to print messages for his perusal. Shoars discovered the tap and subsequently sent a message to the Manager of Network Software and E-Mail Administrator requesting an e-mail account to which Hillseth would not have access. Hillseth intercepted the message and fired her. Shoars filed a $75 million class action suit, *Flanagan v. Epson America, Inc.*, on behalf of herself, about 700 Epson employees, and approximately 1,800 outside the organization, but the court rejected the class certification (Gantt 1995). Shoars also filed a $1 million wrongful discharge suit, *Shoars v. Epson America, Inc.*, claiming Epson had violated California Code by invading its employees' privacy and wrongfully terminating her (Morris 1995). The Los Angeles County Superior Court judge dismissed the lawsuit, ruling California's privacy statutes were not intended to include e-mail. The company's right to intercept messages in the process of managing its systems was recognized. The Shoars case was subsequently filed in the California Court of Appeal, Second Appellate District, which affirmed the decision of the Superior Court (Morris 1995).

In Colorado Springs, Colorado, several of the City Council members became suspicious when the mayor, Robert Isaac, appeared unexpectedly knowledgeable about matters discussed between Council members via e-mail. The mayor admitted reading employees' e-mail messages after the city manager, Roy Pedersen, discovered a secretary printing them and then deleting them to save disk space (Reynolds 1990). The printed copies were maintained in case e-mail was covered by the state's broad public-records law. Colorado Springs, like most local governments in the United States, has open-meeting laws which generally require elected officials to conduct most business on policy matters in public meetings (Bairstow 1990). The mayor thus thought he was appropriately managing the affairs of the city council (Winters 1993). One city councilman

reportedly had considered filing criminal charges against the mayor for allegedly compromising the privacy of the Council members' messages (DeBenedictis 1990). However, no legal action was initiated.

In another example case, Borland International, Inc., of Scotts Valley, California, suspected an employee, Eugene Wang, of divulging trade secrets to his future employer and Borland competitor. Wang was executive vice president of Borland's Computer Languages Division before he left to join Symantec Corp., based in Cupertino, California. On the day he announced his resignation, Borland alleges Wang sent twelve messages, containing confidential information about new software under development, to Symantec's founder and Chief Executive Officer, Gordon Eubanks (Pillar 1993). After Wang left, Borland checked on their suspicions by retrieving stored, but subsequently deleted, outgoing MCI e-mail messages. Borland presented the evidence to the Santa Cruz County District Attorney's Office, which obtained a search warrant. A search of Symantec's offices and Eubanks' two homes confirmed Eubanks received Wang's messages. Borland filed a civil lawsuit, contending Wang had stolen trade secrets. Symantec responded by filing a countersuit contending Borland's lawsuit was an attempt to drive down the price of Symantec's stock. Eubanks was indicted on eleven counts of receiving stolen property and conspiracy; Wang on twenty-one criminal counts of conspiracy and trade-secret law violations. Both pleaded not guilty. The civil case is currently on hold, pending the outcome of the criminal charges (Morris 1995). A key issue will be whether Borland violated the Electronic Communications Privacy Act (ECPA) by accessing e-mail messages from an external system. Borland views access as a property right since it provides each employee with an MCI e-mail account, maintains all account passwords, and pays for the accounts. Borland's position seems consistent with other cases of e-mail privacy invasions on company-provided systems, which were recognized as company property rights. If, as Symantec contends, Borland did indeed violate the privacy of Wang's e-mail, will the confiscated e-mail messages be admissible as evidence in court?

As was the case for Cells 2 and 4 in Figure 1, no legal consequence will result in the absence of a formal e-mail policy, as long as an organization does not monitor e-mail (Cell 6). Thus, it would seem that for an employer who never monitors e-mail, regardless of whether a formal policy has been formulated (Cells 2 and 4) or not (Cell 6), the threat of legal liability is nonexistent. However, organizations are not only confronted with conditions which prevail internally, but must also contend with the complexity of the external environment.

3.4 External Threats to E-mail Communications

The possibility of privacy intrusions from sources external to the organization is a constant threat (Cell 7). Law enforcement agencies investigating illegal activities may present a search warrant granting them access to search organizational property, including e-mail messages in transit, stored on disk or in paper form, backed-up to tape, or even those which have been deleted and overwritten. Similarly, through court discovery processes, a subpoena may be issued to require organizations to comply with requests to examine e-mail in its various forms. Finally, although their activities are illegal, hackers may nonetheless gain access to company records, wreaking unforeseen havoc in their ventures.

Although some employees report awareness that their e-mail messages are not private, they may not be prepared to publicly discuss them. For example, two White House secretaries, Linda Tripp and Deborah Gorham, exchanged comments via e-mail about their respective bosses, former White House counsel Bernard Nussbaum and former White House deputy counsel Vincent W. Foster, Jr. During questioning at the Senate Whitewater hearings, Sen. Christopher J. Dodd (D., Conn.) remarked, "Obviously, neither of you ever imagined, I presume, when you were sending those e-mails, that we would be sitting here talking about it at a congressional hearing" (Cannon 1995). Tripp sheepishly responded that while she was aware that White House e-mail messages were stored, "they weren't intended to be shared" (Cannon 1995). Even casual correspondence becomes a part of the organization's documented internal communications, subject to subpoena.

Corporations generally have paper retention and destruction policies for company records, which are not necessarily applied to computer records. One firm was reported to have indiscriminately backed-up computer records on 22,900 nine-track magnetic tapes containing twenty-five years of company history. During litigation, opposing counsel learned of their existence and obtained a court order to turn over all of them (*The National Law Journal* 1994). Eric Bochner, an attorney for Intuit Inc., aptly stated, "Ninety-eight percent of the documents that companies keep don't need to be kept. But, there is never a spring cleaning day at the office" (Himelstein 1995). His comment was in response to a search of company records, including

approximately 80,000 e-mail messages, to fulfill a 76-page request for data by the Justice Department to analyze a proposed merger of Intuit with Microsoft Corp.

Even in cases where astute employees delete e-mail messages of a questionable nature, the messages may still reside on the system. Perhaps the most infamous example of retrieval of deleted messages occurred during the Iran-Contra investigations (Kallman and Sherizen 1992). Deleted IBM Professional Office System (PROFS) e-mail correspondences between Oliver North and John Poindexter, then National Security Advisor, were retrieved from White House back-up tapes. During testimony at the Senate hearings, Oliver North was quoted as saying, "We all sincerely believed that when we sent a PROFS message to another party and punched the button 'delete' that it was gone forever. Wow, were we wrong!" (National Public Radio 1992).

It is not necessarily only the employee who may be negatively impacted by retrieval of deleted messages. Four female employees received a settlement of $2.2 million from Chevron Corporation for a sexual harassment case. While Chevron denied the charges, the women claimed, among other things, to have been subjected to offensive e-mail messages. Retrieved messages confirmed their claim (Himelstein 1995).

In a $150 million securities fraud case, Siemens Solar Industries contends Atlantic Richfield Co. (ARCO) fraudulently misrepresented the value of their solar energy subsidiary in the sale of the subsidiary to Siemens (*Siemens Solar Industries v. Atlantic Richfield Co*. 1994). Entered into evidence were ten retrieved e-mail messages, sent prior to the acquisition, which Siemens claimed revealed shortcomings of the subsidiary's main product. ARCO claimed the messages were taken out of context and that Siemens was fully informed about the subsidiary. Siemens' federal securities claims were ultimately dismissed as untimely.

In a sexual harassment case, a female employee's boss contended her firing was due to economic considerations. John H. Jessen, of Electronic Evidence Discovery Inc. based in Seattle, expertly recovered an e-mail message which had been deleted by its sender and then overwritten. In this message, the company president wrote to the head of personnel, her direct manager, "I want you to get that tight-[redacted] out of here. I don't care what you have to do." (*The National Law Journal* 1994). The corporation agreed to settle her case for $250,000.

In a trade-secrets allegation, Vermont Microsystems Inc. (VMI) based in Winooski, Vermont, alleged that a program developed for Autodesk Inc. of Sausalito, California, was similar to one a former VMI engineer had created for VMI. The suspicious nature of the engineer's e-mail message content, coupled with permanent file deletions from his hard drive, led a judge to rule in favor of VMI, awarding them $25.5 million in damages (*Vermont Microsystems Inc. v. Autodesk Inc*. 1996).

4. EXAMPLE CASES WITHIN THE UNITED STATE OCCURRING UNDER OTHER CONDITIONS

Factors in the environment and the U.S. legal system are much more complex than the simplistic depiction in Figure 1. All cases of e-mail privacy intrusions will not fit neatly into the cells presented in the framework. Further, for cases settled out-of-court, the facts reported may be incomplete. Even legal cases on record may not provide a comprehensive report of the facts. Thus, the framework is not universally applicable.

An example case which does not fit into the framework is that of an employee who wrongly granted himself the right to monitor e-mail. At the Los Angeles Times Moscow bureau, correspondents became suspicious when they discovered, through the system's log, that entry to their accounts via password had occurred at times they themselves had not logged on (Sims 1993). In a sting operation set up by the newspaper, Michael Hiltzik implicated himself as the intercepter of the messages. It was not reported exactly how the co-workers' passwords were obtained. The Los Angeles Times recalled the correspondent for reassignment to an undisclosed position.

5. CONCLUSION

In the example cases of employee e-mail privacy intrusions discussed, each of the employees whose privacy was intruded had an expectation of privacy. This viewpoint is underscored in a statement by Marc Rotenberg, director of Computer Professionals for Social Responsibility, "E-mail should be treated as private because people use it as if it's private. And that's a very good indication of how our society regards its use" (Ewell 1994). Indicative of the seriousness of this expectation of privacy is the increasing number of cases dealing with compromised e-mail privacy. Currently, the U.S. legal system does not recognize an expectation of privacy for e-mail communications in particular. Surprisingly, the legality of this position was still upheld when an employee was fired for the content of his messages, even though a formal policy explicitly assured e-mail would not be monitored and that such monitoring would not be used against employees *(Smyth v. Pillsbury* 1996). However, the example cases also revealed that the employer may be held financially liable for the content of employee's e-mail. In one case, the company was held liable for the staggering sum of $25.5 million (*Vermont Microsystems v. Autodesk* 1996). Since it is the employer who bears the responsibility to conduct its affairs in an ethically and legally appropriate manner, should the employer retain the right to monitor e-mail?

An obvious conflict exists between employee perceptions of privacy protection and those actually afforded by the U.S. legal system. As demonstrated, e-mail *always* has the potential to be subject to the specter of scrutiny by unintended recipients, resulting in multiple risks for both employers and employees. Given that the existing legal system has not kept pace with technological advances, the responsibility to reduce the risks associated with privacy in e-mail communications falls upon employers and employees alike.

6. REFERENCES

Bairstow, J. "Who Reads Your Electronic Mail?" *Electronic Business*, June 11, 1990, p. 92.

Baumhart, J. T. "The Employer's Right to Read Employee E-mail: Protecting Property or Personal Prying?" *The Labor Lawyer*, Volume 8, Number 4, Fall 1992, pp. 923-948.

Cannon, A. "Whitewater Panel Airs E-Mail Messages." *Philadelphia Inquirer*, August 2, 1995, p. A4.

DeBenedictis, D. J. "E-mail Snoops: Reading Others' Messages May Be Against the Law." *ABA Journal*, September 1990, pp. 26-27.

Ewell, M. "Watch What Your Computer Messages Say." *Philadelphia Inquirer*, May 3, 1994, pp. G1, G4.

Flanagan v. Epson America, Inc., Calif. Super. Ct. No. BC 007036, 3/12/91.

Gantt, L. O. N, II. "An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace." *Harvard Journal of Law & Technology*, Volume 8, Number 2, Spring 1995, pp. 345-425.

Griffin, J. J. "The Monitoring of Electronic Mail in the Private Sector Workplace: An Electronic Assault on Employee Privacy Rights." *Software Law Journal*, IV, 1991, pp. 493-527.

Harper, L. "Mind Your Own Business." *Wall Street Journal*, October 5, 1993, p. A1.

Harvard Law Review. "Addressing the New Hazards of the High Technology Workplace." Volume 104, Number 8, June 1991, pp. 1898-1916.

Hernandez, R. T. "ECPA and Online Computer Privacy." *Federal Communications Law Journal*, Volume 41, Number 1, November 1988, pp. 17-41.

Himelstein, L. "The Snitch in the System." *Business Week*, April 17, 1995, pp. 104-105.

Kallman, E. A., and Sherizen, S. "Private Matters." *Computerworld*, November 23, 1992, pp. 85-87.

Luck v. Southern Pacific Transportation Company, 267 Cal. Rptr. 618 (Ct. App. 1990), *cert. denied*, 111 S. Ct. 344, 1990.

McNeil, H. L. and Kort, R. M. "Discovery of E-Mail and Other Computerized Information." *Arizona Attorney*, April 31, 1995, pp. 16-21.

Morris, F. C., Jr. "E-Mail Communications: The Next Employment Law Nightmare." *American Law Institute— American Bar Association Continuing Legal Education ALI-ABA Course of Study*, August 24, 1995.

Nash, J., and Harrington, M. J. "Who Can Open E-mail?" *Computerworld*, January 4, 1991, pp. 1, 88.

The National Law Journal. "Problems Lurk in Information Boom." May 30, 1994, p. B3.

National Public Radio news broadcasts, 1992.

O'Connor v. Ortega, 480 U.S. 709, 1987.

Office of Technology Assessment (OTA), Federal Government Information Technology: Electronic Surveillance and Civil Liberties, 1985.

Pillar, C. "Special Report on Electronic Privacy: Bosses With X-Ray Eyes." *Macworld*, July 1993, pp. 118, 120.

Restatement (Second) of Torts § 652B (1977).

Reynolds, Chris, "Private and Confidential." *New Scientist*, July 1990, p. 21.

Rose, L., and Wallace, J. *The Sysops Legal Manual*. Winona, MN: 1992, pp. 101-102.

Shoars v. Epson America, Inc. No. SWC 112749 (Cal. Sup. Ct. filed July 30, 1990).

Shoars v. Epson America, Inc. No. BC 007036 (Cal. Sup. Ct. filed March 12, 1991).

Siemens Solar Industries v. Atlantic Richfield Co., WL 86368 (S.D.N.Y.), 1994.

Sims, C. "Reporter Disciplined for Reading His Co-workers' Electronic Mail." *New York Times*, December 6, 1993, p. B9.

Sipior, J. C., and Ward, B. T. "The Ethical and Legal Quandary of E-mail Privacy." *Communications of the ACM*, Volume 38, Number 12, December 1995, pp. 48-54.

Skinner v. Railway Labor Executives Association, 489 U.S. 602 (1989).

Smyth v. The Pillsbury Co. No. Civ. A. 95-5712 United States District Court, January 23, 1996.

Soroka v. Dayton Hudson Corporation, 7 Cal. App. 4th 203, *review granted*, 4 Cal. Rptr. 2d 180 (1992).

Stevens, L. "Mastering E-mail Management." *Datamation*, December 15, 1992, pp. 51-53.

Traynor, M. "Computer E-mail Privacy Issues Unresolved." *The National Law Journal*, January 31, 1994, pp. S2-S4.

Vermont Microsystems Inc. v. Autodesk Inc., 88 F.3D 142, 1996.

Watkins v. L. M. Berry & Company, 704 F2d 577 (11th Cir. 1983).

Wiegner, K. "The Trouble with E-mail." *Working Woman*, April 1992, p. 46.

Wilkinson v. Times Mirror Corporation, 215 Cal. App. 3d 1034 (Cal. App. 1 Dist. 1989)

Winters, S. "The New Privacy Interest: Electronic Mail in the Workplace." *High Technology Law Journal*, Volume 8, Number 1, 1993, pp. 197-233.

ZifNet. "Privacy Issue Comes of Age in the Networked World." *PC Week Special Report*, June 28, 1993, pp. 203-4+.