How private are employees’ email messages? The answer is unclear. This lack of clarity means that protection of employee email will be at the forefront of legal controversy for at least the rest of the decade.

Privacy protection is not a new issue, and employee privacy encompasses a spectrum of issues, including:

- Drug testing;
- Searches of employees and their work areas;
- Psychological testing;
- Telephone, computer, and electronic monitoring; and
- Other types of employee surveillance.

The controversial nature of these areas demands that employers and employees, as well as those with whom they interact—consultants, information service support personnel, suppliers, and customers—be aware of, and responsive to, expectations of and concerns about privacy. Users and organizations naive about ethical conduct and the legal parameters concerning email privacy are vulnerable to harm caused by intrusions. This article examines the potentially conflicting expectations of employers and employees regarding the ethical and legal aspects of privacy invasions in email communications. It also examines the U.S. legal
system to determine the applicability of federal and state constitutional law, state common law, and federal and state statutory sources in protecting email privacy.

Email and Ethics
Organizations have an obligation to their employees, business partners, customers, and society, as well as to themselves, to act ethically. However, ethical behavior is often difficult to achieve. A primary concern is actual or potential harm to individuals and groups. What is ethical and what is unethical? Answers are not straightforward. Societal standards of “good,” “right,” and “moral” help guide our behavior, but do not provide definitive answers for all situations. The political debate on individual and workplace privacy highlights the lack of consensus of opinion with respect to ethics and privacy. Legislatures and courts are being asked to resolve the ethical and legal questions raised by drug testing, physical searches of persons and places, electronic surveillance, and other privacy issues. This article seeks to raise awareness of the ethical issues of email privacy by identifying the vulnerabilities plaguing email and the privacy expectations of employers and employees regarding their use of email.

The increasing number of computer users, applications, and system interconnections, along with the increasing complexity of overall technological capabilities means a greater chance for email privacy to be compromised. Email privacy invasions are characterized along two dimensions: sources of invasion and types of invasion (see Figure 1). Email communications are at risk for interception from sources both internal and external to the organization. Internal sources are people employed by the organization, including executives, managers, and co-workers. External sources are people with whom the organization interacts, through formal and informal relationships. Formal relationships can link service providers, consultants, suppliers, and customers. Interaction may also occur in the absence of formal relationships—with competitors, corporate spies, and hackers.

An invasion may be authorized or unauthorized—that is, it may be condoned by an internal authority, such as a manager, an external authority, such as a law-enforcement agency, or it may be a totally unauthorized privacy violation. These combinations are organized into four cells. This article focuses on internally authorized interception of email messages (cell I in Figure 1).

Employers’ View of Email Privacy
Email monitoring in organizations may be viewed by employers as a necessity, as well as as a right. As owners of the resources, employers may assume the right to monitor email. Such monitoring may or may not be ethically acceptable or legally permissible. But the reasons offered by employers for doing so may appear ethical and legal, including prevention of personal use or abuse of company resources, the prevention or investigation of corporate espionage or theft, cooperation with law-enforcement officials in investigations, the resolution of technical problems, or other special circumstances.

A grayer area is when internal email monitoring is used to track worker performance. In this case, it is not just suspected individuals whose email is read. Hardworking employees might use email to help make a sale or to meet work deadlines; if not for their record of correspondence, their productivity and accomplishments may otherwise go unnoticed.

For publicly traded companies, an employer must ensure that employees abide by Securities and Exchange Commission rules. A company that fails to monitor performance by examining email messages sent to external destinations might be failing to protect trade secrets and proprietary information.

To achieve the positive results in these examples, all messages sent and received by employees would be subject to scrutiny. Some may regard this as an unethical disregard of employee privacy. Information an employee intends to keep private and confidential may be examined. However, an employer could argue that since the email system is owned by the employer and is to be used for the employer’s pur-

Figure 1. Types of employee email privacy invasions
poses, the employee should not expect communications to be private. The employer would conclude that email monitoring is not unethical because employees have no reasonable expectation of privacy with respect to the employer’s email system. Conversely, some may argue that monitoring is indeed an unethical invasion of an individual’s privacy in light of the potential for negative consequences.

Monitoring can be a double-edged sword for those being monitored. Productive and exceptional employees, as well as employees who are unproductive, could be readily identified throughout the organization.

**Employees’ View of Email Privacy**

From the employees’ perspective, the content—even the existence—of email messages may be regarded as confidential, private correspondence between sender and receiver(s). This perception seems reasonable, given that email is accessed as a facility in users’ computer accounts, to which access is password-controlled, providing a sense of confidentiality. Further, most people are familiar with the privacy protection of the U.S. mail and may assume it applies to email as well. Thus, users can mistakenly and reasonably assume that email messages are free from interception.

Electronic surveillance for the purpose of improving job performance, product quality, and productivity takes many forms. For example, email messages are usually sent and received in directly readable, unencrypted alphanumeric form, intended for immediate reading. Employee computer screens may be viewed or messages may be intercepted without employee knowledge or consent. Email messages are thus exposed to employer scrutiny. At Epson America, Inc., an email system administrator, Alana Shoars, claimed to have been terminated in 1991 for protesting the routine practice of intercepting and printing employees’ MCI email. In her case, Shoars vs. Epson America, Inc., she claimed Epson’s invasion of privacy and her termination violated California law [16]. In another 1991 case, Bourke vs. Nissan Motor Corp., two software specialists contend they were forced to quit after a supervisor read their personal email correspondence, which included sexual statements [3]. They also claimed invasion of privacy and wrongful termination in violation of California law.

In both cases, the companies’ right to manage their email systems was legally recognized. But because both were tried in lower-level California state courts and have not yet worked their way through the appellate process, they are of minimal value as precedents. The question remains: Were the companies’ actions ethical?

Many users expect that when they press the delete key on their computers, an email message is actually deleted. However, user deletions are often archived on tape and stored for years. For example, a former employee of Borland International, Inc. found, to his dismay, that deleted messages can be retrieved from the archives [14]. The employee was suspected of using a Borland-supplied MCI email account to divulge trade secrets to his future employer—and Borland rival—Symantec Corp. Borland asked MCI Communications Corp. to retrieve the former employee’s deleted messages. This alleged intrusion was viewed as a property right by Borland. Since Borland paid for the email service, the employee’s account became Borland’s property upon his departure. The result: pending criminal investigations of both the sender and recipient, as well as a civil suit, Borland vs. Symantec.

Perhaps the most infamous example of retrieval of deleted messages occurred in 1987–89 during Congress’s Iran-Contra investigations. Deleted IBM PROFS email correspondences between Oliver North and John Poindexter were retrieved from White House backup tapes. In testimony before the Senate, North said, “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.” [9].

Regardless of the type or characteristics of email system used, the question remains: what privacy protection, if any, does an employee have in email communications? Such communications are usually made on the employer’s premises, with the employer’s equipment, on the employer’s time, and at the employer’s cost—to further the employer’s objectives. With such a substantial employer investment, do employees have a legitimate expectation of email privacy?

Despite employers’ significant proprietary interests, employees do have expectations of privacy [10]. Given the potentially differing perceptions of employers and employees regarding email privacy and the potential problems that can result from privacy intrusions, employees and employers both need to understand the privacy protection provided by the U.S. legal system. Although ethics and law are not identical, they do come in close contact. Law is often the vehicle for formally implementing ethics into social guidelines and procedures.

**Legal Protection of Email Privacy**

What is privacy? The U.S. concept of privacy has been evolving since the country was founded. The growth of cities, accompanied by improved communication technologies and migration from more isolated rural environments, changed the national concept of privacy. Explicit legal recognition of U.S. privacy rights did not exist until the late 1800s [21]. Although privacy rights were then recognized, the extent of these rights remained unclear. Almost 40 years ago, a federal judge described the confusing state of privacy rights as a “haystack in a hurricane” [4]. In an often–cited 1964 article [2], Edward J. Bloustein, a law professor at New York University School of Law, wrote that “words we use to identify and describe basic human values are necessarily vague and ill-defined.” He regarded individual
privacy as, in part, a spiritual issue, the invasion of which is an affront to individuality and human dignity.

Is the monitoring of an employee’s email such an affront to individual human dignity as to be prohibited by law? What is an employee’s reasonable expectation of privacy? There are no definitive answers. The scope of privacy protection depends on the legal source being consulted. Therefore, the reasonableness of employee expectations of privacy varies, depending on whether the claim is made under constitutional, common, or statutory law. Resolution of the issue requires balancing the employer’s property rights and the employee’s reasonable expectation of privacy.

Because email is a relatively new form of commercial communication, it lacks extensive legal precedents to define the parameters of privacy associated with its use. Technological progress proceeds more quickly than the law. Issues of email privacy must be assessed through protections established for employee privacy in general and through three elements of the U.S. legal system:

- U.S. and state constitutional law;
- State common law; and
- Federal and state statutory protections.

However, none specifically address email monitoring. Can legal sources that protect privacy in general provide privacy protection for email communications in particular? The following analysis, summarized in Table 1, concludes that none seem to protect the privacy of employees in their email communications.

**U.S. Constitutional Privacy Protection.** The U.S. Constitution, in part, defines the relationship between the U.S. government and its citizens. Protection of public-sector employee privacy is provided through the Constitution and the various state constitutions. For example, the Fourth Amendment 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” seem to include all employees, neither the Fourth Amendment nor any other part of the Constitution protects the privacy interests of private-sector employees. Usually, only public-sector employees of federal, state, and local governments have privacy protection under the Constitution [5]. Constitutional protection can be extended to private-sector employees if they demonstrate sufficient governmental involvement, referred to as “state action” [17]. U.S. Supreme Court decisions regarding privacy rights of public-sector employees based on the Fourth Amendment may influence state and federal court decisions.

Public-sector employees’ privacy protection under the Fourth Amendment is not unlimited. For example, a Supreme Court case dealing specifically with a public employee’s privacy in the workplace, *O’Connor vs. Ortega* [11], involved the firing of Mango Ortega, a psychiatrist in a state hospital, as a result of an investigation of alleged impropriety that included the search of his locked office, desk, and file cabinets. Ortega sued the hospital, claiming his Fourth Amendment right to privacy was violated by the search.

After the case worked its way through the courts, the Supreme Court rendered a decision based on two points:

- Whether or not Ortega had a reasonable expectation of privacy; and

<table>
<thead>
<tr>
<th>Legal Protection</th>
<th>Interpretation for Email</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Constitutional</strong></td>
<td>Generally, only public-sector employees of federal, state, and local governments have limited privacy protection. To date, there is no precedent for email.</td>
</tr>
<tr>
<td>- U.S. Constitution’s Fourth Amendment</td>
<td></td>
</tr>
<tr>
<td>- State Constitutions</td>
<td>Privacy protections vary substantially from state to state. California has the most developed state constitutional privacy protection. The effect on email is unclear.</td>
</tr>
<tr>
<td><strong>State Common Law</strong></td>
<td>Evolving through state court decisions, email privacy protection, if any, is contained in the tort of invasion of privacy and the causes of action related to this tort.</td>
</tr>
<tr>
<td><strong>Statutory</strong></td>
<td>Not much federal or state legislation has addressed email privacy.</td>
</tr>
<tr>
<td>- Federal Statutes</td>
<td>Exceptions included in this law apparently leave employee email privacy unprotected.</td>
</tr>
<tr>
<td>Electronic Communications Privacy Act (ECPA) of 1986</td>
<td>Since 1991, this proposed law has been debated in both the U.S. Senate and the House of Representatives.</td>
</tr>
<tr>
<td>Proposed Privacy for Consumers and Workers Act</td>
<td>Privacy protections, if any, vary from state to state. Regulation is primarily at the federal level through the ECPA. States can enact statutes more stringent than the federal statute.</td>
</tr>
<tr>
<td>- State Statutes</td>
<td></td>
</tr>
</tbody>
</table>
• Whether or not the search of his office was unreasonable.

On the first point, the Court held that since Ortega had a private office, he had a reasonable expectation of privacy. However, the Court also found the search of his office to be reasonable because 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. Since work environments vary, a public-sector employee’s expectation of privacy must be determined on a case-by-case basis.

Factors the Court considered included notice to employees, exclusive possession by an employee of keys to a desk or file cabinet, the government’s need for access to documents, and the government’s need to protect records and property [1, 5].

With respect to email, the extent of constitutional protection is unclear. Email is not like a locked desk or file cabinet. The employer has access to all messages on the system. It could be argued that with respect to email, the public-sector employee’s legitimate expectations of privacy are diminished.

State Constitutional Privacy Protection. Some state constitutions specifically grant individuals an explicit right to privacy [1, 5]. This right usually extends to protection from the actions of state governments, not private organizations. However, in 1972, California amended Article I, Section 1 of its state constitution to include privacy protections. A California appellate court then held that the state’s right of privacy applied to both public- and private-sector interests [23]. Further, in Soroka vs. Dayton Hudson Corp. [18], the California Court of Appeals reaffirmed this view, holding that an employer may not invade the privacy of its employees absent a compelling interest.

In Soroka, the invasive action of the employer was the administration of a psychological screening test for job applicants. Similarly, some compulsory employee drug testing has been held to violate California’s constitutional right to privacy [8]. However, it could be argued email surveillance is different from drug and psychological testing; email is part of a network to which others have access, and therefore may not be subject to the same privacy right. Conversely, it could be argued even if an employee is aware of actual or potential email monitoring, the California privacy right may still apply. Under the California Constitution, the right is not based on employees’ reasonable expectations of privacy, but on employers’ compelling interests, sufficient to invade employee privacy [7]. How this applies to email, or even if it applies, remains to be decided.

State Common-Law Privacy Protection. Since the privacy of most employee email communications is not protected by the Constitution or by most state constitutions, does common-law privacy protection apply? Common law is a continuously changing system of law, developed and updated by judicial decisions based on societal values, customs, and usage, rather than on codified written laws, known as statutory law. The common-law privacy claim most likely to be asserted in response to the monitoring of an employee’s email is the tort of invasion of privacy, more specifically, intrusion upon seclusion [5]. This theory views privacy as based broadly on concepts of individual human dignity and respect, rather than as a separate independent value [6]. Generally, the courts have narrowly construed employee privacy rights and seemed reluctant to expand such privacy protection. Employee claims based on common-law invasions of privacy are not usually successful [5].

To apply the tort of inclusion upon seclusion to email privacy, an employee whose email is covertly monitored must demonstrate three things:

• An intrusion;
• An intrusion into a private affair or concern; and
• That the intrusion would be highly offensive to a reasonable person [13].

Undisclosed monitoring of email would seem to be an intrusion, but are messages on an employer’s email system a private affair or concern? Since the system is for the employer’s business purposes, is there also a reasonable expectation of privacy? The answer is unclear, but the courts have extended privacy protection to the analogous areas of wiretapping telephone calls and intercepting written communications [5]. Further, the same rationale would seem to apply to the third element—whether email monitoring would be highly offensive to a reasonable person. This monitoring is done on equipment owned by the employer and is 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 the question of whether this tort applies to the monitoring of email. Since email users are usually given secret passwords, employee expectations of privacy may be elevated. Employees may legitimately consider email in the context of the telephone and the U.S. mail. It has been held that the unauthorized opening of an employee’s mail creates a cause of action for invasion of privacy. The Third Circuit Court of Appeals reasoned that in the absence of authorization, employees may reasonably expect that their private telephone conversations would not be intercepted, nor would their private mail be opened [20]. Does this reasoning apply to email? The courts have been reluctant to make this judicial extension [6]. Employee claims arising from common-law invasion of privacy are generally unsuccessful with respect to email monitoring, primarily because such monitoring does not affect any legally recognized individual privacy interest [5].
Federal Statutory Privacy Protection. Constitutional law and common-law protections of email privacy are vague, at best. As part of the heated ethical and political debate over privacy issues, certain specific statutory protections have been enacted or proposed by Congress. Does this resolve the ethical issues? At best, the legislative process is a means for accommodating conflicting ethical perspectives on an issue. The issue of email privacy is undergoing this process.

Electronic Communications Privacy Act
In an influential 1985 study, the Congressional Office of Technological Assessment (OTA) found approximately 50% of the U.S. population believed computers threaten privacy rights and supported further action to protect these rights [10]. This study inspired Congress to enact the Electronic Communications Privacy Act (ECPA) of 1986 [19]. As a society, Americans generally value privacy. However, if a societal value, such as personal privacy, is not legally protected, is it a right? By implication, the American people seem to assume they are already endowed with this right. With respect to email, the OTA stated “the existing protections are weak, ambiguous, or nonexistent” [10]. This lack of protection is significant because email is vulnerable to interception, as identified by the OTA, at five specific stages:

- At the sender’s terminal or electronic file;
- While being transmitted;
- When accessing the recipient’s mailbox;
- When the communication is printed in hard copy; and
- When retained in the files of the email service.

Relying on the 1985 study, the OTA concluded internal company email systems were not covered by federal statute [10]. Congress used the ECPA to amend existing federal wiretap protection law to include most electronic communications. Its purpose was to extend privacy protections against wiretapping to new forms of electronic communications, including email, cellular telephones, and data transmission, from improper interception.

Broadly, the ECPA prohibits interception of wire, oral, and electronic communications, as well as disclosure or use of such intercepted communications. The statute’s broad definition of electronic communication includes email. Further, in Title II, the ECPA, subject to significant exceptions, prohibits access to and disclosure of stored electronic communications.

Two Exceptions
Whether coverage extends to monitoring the email of private-sector employers is unclear because of two exceptions in the ECPA that were part of earlier federal wiretap protection law:

Business Use or Business Extension. This exception is the basis for most of the cases brought under the ECPA [5]. To be an effective defense against employee claims of email privacy invasion, employers must demonstrate that a business use was the reason for the interception and that monitoring was conducted within the ordinary course of business [22]. In a 1983 case [22], brought under the prior federal wiretap protection law, an employer notified an 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 the telephone communication was personal. This exception, which can be applied to telephone communications, would seem to apply to email. If an employer wants to ensure its email system is used solely for work-related purposes, routine monitoring of the content of email messages might be included under this exception.

Prior Consent. This exception may permit telephone and email monitoring. Under it, employers may be able to protect themselves against the risk of liability by notifying employees their email may be examined. Such consent may be express or implied but is limited to the scope of the consent. In the aforementioned 1983 case, the consent was only to the monitoring of business calls. The court refused to extend this consent to all telephone calls.

The issue of whether the ECPA protects the privacy of email is unclear and is currently under debate in the courts. A review of relevant legal research seems to conclude that the ECPA does not afford significant privacy protection to employee email communications [5, 6].

Proposed Legislation
Email and other computer technology has changed faster than the law. Law usually reacts to pressures in society more slowly than technology reacts to such pressures. To further protect individual employee privacy interests, the Privacy for Consumers and Workers Act [12] was introduced in 1991 in both the Senate and the House of Representatives. To date, it has not been enacted but was reintroduced in 1993 by Senator Paul Simon, Democrat of Illinois, in the Senate and by Representative Patrick Williams, Democrat of Montana, in the House of Representatives.

This proposed legislation would prevent perceived abuses of electronic monitoring in the workplace. It requires employers do three things:

...if a societal value, such as personal privacy, is not legally protected, is it a right?
• Provide advance written notification to employees if email messages or computer keystrokes are to be monitored;
• Notify employees of any monitoring policies; and
• Disclose entry into an employee’s hard drive after the fact.

An employer would be allowed to monitor an employee without notice—if there is “reasonable suspicion that any employee is engaged in conduct which (A) violates criminal or civil law or constitutes willful gross misconduct, and (B) adversely affects the employer’s interests or the interests of such employer’s employees” [12]. If enacted, this legislation could significantly restrict an employer’s ability to legally monitor employees’ email.

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 address these issues through either wiretapping legislation or electronic monitoring legislation or both [5]. Generally, these efforts are not effective in protecting the privacy of employee email.

An attempt was made in the original 1990 Shoars vs. Epson America, Inc. case to find employee email privacy protection in California’s criminal laws [15]. California Penal Code Section 630 prohibits wiretapping without the consent of all parties involved, adding 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 judge in the California Superior Court dismissed the lawsuit, ruling that Section 630 did not apply since the legislation did not specifically refer to email. However, an amended complaint alleging a civil cause of action was filed later in 1991 [16].

Conclusions
Various courts and legislative bodies have sought to balance employees’ expectations of personal privacy with employers’ proprietary and access interests. From a managerial perspective, email—an increasingly important organizational resource touted as contributing to worker productivity—must be used in an ethical and legal manner. Since clear guidance is not provided by our legal system, organizations must formulate their own internal email privacy policies. Lacking a formal policy, employee expectations of privacy may differ from their employers’ perspectives. Even with a formal policy, this balance is not easily achieved because of the dynamic nature of information technology capabilities. The rapid pace of technological advances forces the legal system to resolve conflicts for which there is no precedent.

References
1. Bauman, J.T. The employer’s right to read employee email: Protecting property or personal prying? The Labor Lawyer 8, 4 (Fall 1992), 923–948.

Full citations to laws and court cases are available and are only omitted to comply with Communications of the ACM requirements.

About the Authors:
JANICE C. SIPIOR is an associate professor in the Management Department, College of Commerce and Finance, Villanova University. Her research interests include expert systems, system development strategies, and the legal aspects of information technology. Author’s Present Address: Villanova University, 800 Lancaster Ave., Villanova, PA 19085; (610) 519-4347; email: sipior@ucis.vill.edu

BURK T. WARD is an associate professor in the Business Law Department and The Graduate Tax Program at the College of Commerce and Finance, Villanova University. His current research interests include the legal aspects of information technology, estate planning, and business succession planning. Author’s Present Address: Villanova University, 800 Lancaster Ave., Villanova, PA 19085; (610) 519-4375; email: bward@ucis.vill.edu

© ACM 0002-0782/95/1200 $3.50