Electronic Mail, Privacy and the Public Sector: Guidelines for Public Employees and Organizations

By

Charles M. Schweik

* Paper presented at the Workshop in Political Theory and Policy Analysis Mini-Conference, May 1-3, 1993.

Abstract

What privacy rights are public employees entitled to when using their electronic mail systems? Are they entitled to privacy rights in the messages they send or receive? Or is it the case that they have no privacy rights to these messages whatsoever? Could it be that all information which resides in a public organization's computer system simply be the property of the organization? Unfortunately, no public sector electronic mail privacy case has been considered by the courts, but that does not mean E-mail privacy guidance does not exist. After a discussion on different interpretations of privacy, and a consideration of language's influence on its interpretation, the paper provides a summary of privacy provisions provided by the United States Constitution. The paper then investigates previous privacy considerations provided in other workplace situations - cases which involve technologies other than E-mail — in search for common rules established by the Supreme Court. With this foundation, the paper then applies the same rules to an electronic mail environment and provides guidelines intended to assist public employees in the creation or reevaluation of their organization's electronic mail privacy policy.

Introduction

Electronic mail (E-mail) has revolutionized the way organizations communicate. E-mail is a communication system which allows a computer user to send messages to another person's computer terminal at a different location (Droke, 1992, p. 169). E-mail systems usually require some type of user identification (usually referred to as a "userid" and a user password) to gain access to the system. Through this identification procedure, the system provides a control mechanism against unauthorized access. It also provides the user with a unique "mailbox" to which electronic messages can be sent[1] (Droke, 1992, p. 169). The use of E-mail has mushroomed since its inception. It has been estimated that by 1995 more than forty billion E-mail messages will be sent annually and by the year 2000 this number is predicted to reach over sixty billion (Clucky, 1988).

Unfortunately, the rapid diffusion of E-mail has resulted in recent reports of what many would regard as misuses of the technology. Consider the following example:

A secretary for the City of Colorado Springs, Colorado, was required to periodically print out all E-mail messages stored on the city computer and then delete the messages from the system, in order to save computer space. The mayor of the city requested to see these printouts, to ensure that the city council members weren't meeting secretly, using electronic messaging. For nearly a year the mayor monitored the city council member's E-mail activity, without their knowledge. The members of the city council became curious as to how the mayor was consistently so well informed on their views concerning issues they were debating. After being questioned, the mayor admitted to the monitoring of the messages. One member of the council was so upset about what he considered an invasion of privacy that he considered filing criminal charges. He later changed his mind (DeBenedictis, 1990).

If the predictions of increased use of E-mail are accurate, cases of E-mail invasion will undoubtedly increase in the public sector[2] as well as the private sector. Yet up to now, very few E-mail intercepting[3] cases have been considered in a court of law (DeBenedictis, 1990, p. 26). All the cases that have reached the court system have been E-mail intrusion cases from the private sector. This fact, that no public sector cases have been deliberated, is a key point, for issues of privacy in public sector situations can be interpreted differently by the courts. The intent of this paper is to analyze the differences a public setting brings to E-mail privacy, and to provide public managers with guidelines to aid them in developing a sound E-mail policy for their organizations.

A Fictional Public Sector E-mail Invasion Case: A Point of Departure

It is doubtful that many future public sector E-mail access cases will involve actors such as mayors and city council members. A more likely scenario would involve a public sector manager and one or more public employees. For purposes of analysis, suppose we take the facts of the Colorado Springs case and place them in a slightly modified setting:

Suppose instead of the mayor accessing archived E-mail, it is a public sector manager (referred to hereafter as "the manager"). Suppose that the E-mail the manager has been reading was written or received by her employee (referred hereafter as "the employee"). Suppose as well that after a year of this activity, the employee finds out that the access has taken place, feels his or her rights have been violated and decides to take the issue to court. What factors then would the courts use to reach their conclusion? What could have been done *a priori* by the public organization to ensure that a lawsuit never arises?

To answer these questions, this paper relies on this fictional scenario to first define the concept of privacy in an E-mail environment. The paper considers the role of language as it is used to define privacy and as it may influence the way players in a privacy debate (managers or employees! may use language to argue their case. The discussion then turns to an investigation of the rules established by the U.S. courts regarding technologies that have similar privacy properties to E-mail. These will provide insight into how privacy is interpreted in a public sector setting. Lessons are then applied to this fictional E-mail case and the paper concludes with some organizational guidelines based on this analysis.

How Has Privacy Been Violated?

Prior to any analysis of what privacy rights a public employee may have in our fictional case, a common understanding of privacy must be established. Once defined, it would be helpful to consider E-mail privacy from the point of view of the individual employee and the individual employer. In addition, and most importantly, the provisions of the right to privacy in the United States Constitution will be explored as they pertain to our fictional case.

The Right to Privacy: A Definition

The word privacy is commonly understood to signify "the quality or state of being apart from company or observation" or "freedom from unauthorized intrusion" (Webster, 1988). There are other definitions which convey much the same idea. Supreme Court Justice Louis D. Brandeis defined it as "the right to be left alone" *(Olmstead v. United States,* 1928, p. 478). Stephen Rohde, in his in-depth discussion on the origins of the right to privacy, agrees with Brandeis' interpretation but adds that privacy is the right to "be free from unwarranted intrusion in our private lives" (Rohde, 1988). These definitions could be applied to an E-mail setting, but there are two other definitions which are probably more applicable to an E-mail invasion case. The first simply is the right not to have government intrusion (American Enterprise for Public Policy Research, 1979, p. 4); this will be discussed in the section on constitutional provisions below. The second appropriate definition is found in Alan Westin's book Privacy and Freedom. Westin states: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967, p. 7). It is in these meanings, the right of the employee to determine what information is communicated to the manager and the right *not* to have government intrusion, that privacy may have been violated in our fictional case.

The Right to Privacy: The Importance of an Awareness of Language

Crucial to the understanding of privacy rights is a realization of the subtleties language imposes in our interpretation of actions. The ability to analyze and understand actions taken by managers is very much influenced by the established understanding of the term used to describe the action. The analyst must take into account terminology used both from the perspective of its "common definition" as well as what connotations it may bring to the action it describes. For instance, in describing the action taken by a manager in an E-mail case, one could refer to it as "E-mail monitoring." Another person may refer to it as "E-mail invasion" or "E-mail tampering." The term "monitoring" has a much more mild connotation than does either "invasion" or "tampering." A "monitoring" situation implies some sort of agreement in the action that was taking place; that the employee understands that the manager may read E-mail and no privacy issues should arise. A situation described as a "tampering" or "invasion" type of action implies an action which may have been taken without an employee's knowledge. Privacy may very well be violated in a case described by these terms. It is critical that in the investigation to determine guidelines for organizational E-mail privacy we maintain an awareness of the subtle

connotations of the language used to describe the situation. This point is crucial as well to the understanding of the viewpoints of privacy between the manager and the employee - one person's "intrusion" may be another person's "monitoring". These different terms are central to the organizational conflict that may result. To establish a common language with no connotations, the term "access" will be used throughout the paper as a neutral term for E-mail invasion or monitoring.

The Right to Privacy: The Employee's Perspective - "Intrusion"

What would the employee in our fictional case *expect* regarding his or her privacy when using E-mail? To understand how to avoid organizational conflict over E-mail, it is important to try to understand E-mail privacy from the perspective of the employee. Wald and Kahn contend that public employees have "privacy interests in their words, both oral and written, that are not related to their work" (Wald and Kahn, 1990, p. 302). They may even have privacy interests when they communicate about their work.[4]

In his analysis of privacy, Westin points out that privacy performs several functions in a democratic society. The "emotional release" function may be appropriate to an E-mail environment, for it describes periods of privacy which individuals require to vent their frustrations. These "safety-valve releases" provide an outlet for the individual to expel anger at "the system" or "the boss" and may be conducted totally alone or with friends and family (Westin, 1967, pp. 34-35). An employee who uses E-mail as a communication vehicle to a co-worker who is also a friend may assume the E-mail system provides a private atmosphere for releasing this frustration. A manager who accesses E-mail conversations may discover an employee's message of "emotional release." Should the employee find out about this E-mail access, he or she may feel strongly that privacy rights have been violated.

Westin describes a second function of privacy, what he terms the "self-evaluation" function. Self-evaluation is described as a process where "every individual needs to integrate his experiences into a meaningful pattern and to exert his individuality on events." Westin stresses that privacy is essential in this process, by providing time in which the individual can anticipate, originate and refashion ideas. This role of privacy provides time for evaluation, a time where the individual makes the decision "to move from private reflection or intimate conversation to a more general publication of acts or thoughts." Westin stresses the importance of this privacy by saying: "Given the delicacy of a person's relations with intimates and associates, deciding when and to what extent to disclose facts about himself - and to put others in the position of receiving such confidences — is a matter of enormous concern in personal interaction, almost as important as whether to disclose at all" (Westin, 1967, p. 37).

In our fictional case, the manager's actions may be interpreted as an "intrusion" in on the employee's need for self-evaluation. The E-mail communication that was read may have contained thoughts not yet thoroughly developed. The release of the information from employee to manager may have been premature because these thoughts may have been ones that the employee was not ready or prepared for the manager to hear. In sum, E-mail messages involving emotional release and self-evaluation provide examples of the types of information, if intercepted, that may be *perceived* by employees as an invasion of privacy. This monitoring, to the public employee, may be interpreted as a breach of his or her legal rights-- "an invasion". These interpretations, whether founded or unfounded, may lead to organizational conflict.

The Right to Privacy:
The Manager's Perspective — "Monitoring"

A primary argument for the legality of E-mail invasion from a public manager's perspective is in regard to the property rights of the system. In most cases the public organization, as owner, should have rights to all equipment, buildings and information held in its computer systems. From the view point of the manager, the computer system is organization property and consequently everything it contains is the organization's property as well. The manager may feel that he or she has every right to "monitor" the system. This argument is a strong one. One problem however is that most E-mail systems require their users to access the system via a personally assigned password. Thus, whether the manager likes it or not, the personal locking (password) capability of an E-mail system may result in the employees having a subjective expectation of privacy - regardless of the fact that the organization owns the system (Droke, 1992, p. 184; Witt, 1992, p.555). The ownership contention is an important consideration, but it does not change the *expectations* of privacy an employee in the workplace may have.

A second justification for E-mail "monitoring" from a manager's perspective is "business need." A manager may have to access an employee's E-mail in a situation where the employee is absent and his or her E-mail contains some needed work-related information. This is an important point which will be considered in later analysis.

The Right to Privacy:
A Constitutional Perspectives

While an understanding of employee and manager perspectives on E-mail is crucial to avoid organizational conflict, the most important aspect to consider is in respect to the provisions about

privacy in the United States Constitution. The privacy that an employee expects to receive and the constitutional provisions provided to him or her are not necessarily the same. In addition, a clarification should be provided as to why U.S. Constitutional principles are applied in the public sector setting, while they do not apply in a similar private sector setting. Let us first address privacy as it has been interpreted from the Constitution, and then explain why it is appropriate in a public sector E-mail situation.

Privacy, the Citizen and the "Government as Intruder"

The concept of privacy is not specifically addressed in the Constitution (McClellan, 1976 , p. 14). The Supreme Court, in its holding in the case *Griswold v. Connecticut* (1965), concluded that the narrow protections for privacy derived from many of the amendments to the Constitution, taken as a whole, form a "penumbra" guaranteeing privacy (McClellan, 1976, p. 14).

Rohde (1988) agrees, arguing that the lack of discussion about privacy in the Constitution is understandable. "[P]rivacy was such a pervasive and important value to the Founding Fathers, it would no more have dawned on them to spell out its protection in the Constitution than to express the fundamental rule of Anglo-Saxon law that man is innocent until proven guilty - a doctrine which is nowhere mentioned in the Constitution or Bill of Rights" (Rohde, 1988, p. 52). Rohde suggests that the authors of the Constitution were very much influenced by natural rights theories - principles which held that people possess inalienable rights that make them part of the human race. If one then believes that the Constitution and the Bill of Rights flow directly from these theories in which privacy is so well respected, Rohde suggests that after reading the language of these documents one cannot help but conclude that the authors intended citizens of the United States to enjoy the right of privacy (Rohde, 1988, p. 53). Privacy in Rhodes' interpretation is defined as the right of the citizen or individual *not* to have government[5] intrusion.

Privacy, "the Government as Employer" versus "the Government as Intruder"

This returns us to our earlier discussion; the definition of privacy as the right to no "government intrusion." Often in a public workplace a manager may "monitor" or "access" an employee's conversation (written or verbal) in order to perform internal operations of the organization. In other circumstances, the manager may "intrude" into the employee's communication in an effort to "capture" some information. In either instance, the employee is provided with Constitutional protection for the employer, *working as the government,* is acting as intruder[6]. This is a critical point to this analysis, for "government intrusion" now moves beyond an individual's home into the individual's public sector

workplace, and with it Fourth Amendment[7] protections follow. This Amendment provides two aspects of employee protections: it protects an individual's subjective or perceived expectation of privacy and requires that the employer conduct a search only when the search is "reasonable" (Duffy, Pepe and Gross, 1987). In this context, "reasonable" is defined as something that would *not* be found as offensive to a reasonable (or average) person. In a private sector setting, privacy is much more limited because the Constitution protects only against actions performed by a government actor; it does not protect against privacy intrusion of private parties on other private parties (Furfaro and Josephson, 1990, p. 3). Privacy, in the eyes of the courts, are deliberated very differently when the case setting involves a government organization.

What Lessons Can We Learn From Other Privacy Cases?

As stated previously, there have been no public sector E-mail privacy cases deliberated by the U.S. courts. This fact does not mean that a public organization is without guidance in trying to develop a sound E-mail policy. Other public sector privacy cases, specifically cases involving wiretapping or workplace search and seizure, involve privacy issues very similar to our fictional E-mail case. An analysis of the Court's logic in deliberation of these cases will provide significant insight into what is important in regard to public employee privacy.

Wiretapping Cases:

The facts in our fictional E-mail monitoring case are arguably very similar to wiretapping cases for one could say that the E-mail messages were intercepted in transmission to their recipients. The question could be asked, in terms of privacy, what is the difference between the case where a manager intercepts an E-mail message between two people and one where a manager intercepts oral communication (what is commonly called "wiretapping") between two parties on a telephone call? Other than hearing tone of voice (which could produce very different meanings from those of a written message), I would argue that there really is no difference.

Suppose the employee's manager was monitoring not E-mail, but rather employee telephone conversations. Would the courts find that the intrusion violates the employee's Fourth Amendment rights? What would the courts take into consideration to come to their decision? Past wiretapping cases could very well provide insight into how an E-mail case might be considered.

The Federal Wiretap Act: Some Guidelines Established

Privacy rights of telephone conversations in both public and private sectors are regulated by Title III of the Omnibus Crime Control and Safe Streets Act, often referred to as "the Federal Wiretap Act." Congress created the Act in 1968, in response to the perceived need to provide law enforcement officials with the means to investigate organized crime (Clukey, 1988: p. 246). Although this Act prohibited any person from intentionally intercepting a wire or oral communication, it did provide employers, both private and public, two workplace exceptions: first, an employer could establish a prior consent to monitoring agreement with employees and second, phone extensions were not considered a wiretap "device."[8]

The first exception, prior consent, provided in section 2511(2)(d), states that it is not unlawful for a person to intercept wire or oral communications when one of the parties to the communication has provided prior consent, unless intercepted under "color of law or for a criminal or tortious purpose." Consequently, many employers require their new employees to agree to monitoring as a condition of employment (Furfaro and Josephson, 1990, p. 3). Allegations of illegal employer wiretapping have been dismissed due to the fact that employees had been notified that monitoring could occur.[9]

There is an important exception to the rights a manager obtains by prior consent. In *Watkins v. L M. Berry & Company* (1983), the Eleventh Circuit concluded that:

> [A] personal call may not be intercepted in the ordinary course of business... except to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not. In other words, a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents.[10]

Watkins was informed that her telephone calls would be monitored, but only to the extent necessary to determine whether the call was of a business or personal nature. One afternoon, the plaintiff's supervisor listened in on a call in which Watkins discussed plans to interview for another employment opportunity outside of the company. The supervisor reported this finding to upper management and later Watkins took action against this invasion. The court held that even in a case where prior consent to monitoring has been received, once the employer comes to the realization that the conversation is private in nature, the employer is obligated to cease the monitoring and minimize the intrusion. The case was remanded for trial to determine whether the supervisor had monitored the call longer than necessary (Fishman, 1990, p. 196).

in their discussion of what constitutes a monitoring apparatus,[11] Congress specifically excluded telephone devices that are furnished by an electronic communication service and are used by a subscriber in day-to-day business activities. Extension telephones, therefore, do not constitute an interception device in the eyes of Congress. Furfaro and Josephson warn; however, that "[i]n applying the business extension exemption, most courts have narrowly construed the requirement that the telephone system has to be used by an employer in the 'ordinary course' of business" (1990, p. 32).

James v. Newspaper Agency Corporation provides an example of a legal use of an extension telephone for employee monitoring and the importance of "the ordinary course of business." The employer requested that the telephone company install a system which would provide a method to monitor employees' calls. The company wanted the mechanism installed so that managers could assist in the training of employees (who were learning how to conduct phone advertising,} and to protect employees from abusive calls. In dismissing the employee's allegation that the monitoring was illegal, the court held that the extension telephone would qualify under the exemptions, reasoning that the system was installed by the telephone company, the employees had given prior consent to the monitoring, and the employer provided legitimate business reasons for the monitoring (Furfaro and Josephson, 1990, p. 32).

In 1986, Congress realized that some aspects of the Federal Wiretap Act were obsolete due to new technological developments. Consequently, they created the Electronic Communications Privacy Act (ECPA), an amendment to the Federal Wiretap Act, which extended its provisions to cover computer communication (Hernandez, 1988, p. 29). In addition, the ECPA provided protection of communications stored after transmission, such as E-mail filed in a computer electronic mailbox, awaiting the recipient's access. The Act also established exemption to the person or entity providing a wire or electronic communications service from any offenses regarding stored communications. That is, there is no ECPA violation if the owner of the computer network intentionally examines all E-mail on the system (Hernandez, 1988, p. 39). This suggests that some of the manager perceptions on ownership described earlier may be correct; if employers are is the providers of the E-mail system, they can read any employee E-mail that is transmitted within their organizations. At this point, all of the cases that cite the ECPA have involved the use of cellular telephones, not E-mail (Droke, 1992, p. 173). In addition, it is unclear whether the Act is intended to cover public sector environments. Witt (1992, p. 50) states that a review of the legislative history of the Act "indicates that Congress intended the Act to cover private corporate communication systems." Its applicability in a public sector environment may be questionable.

The discussion above leads to the conclusion that, in the case of wiretapping, the determination of the legality of the employer's access would depend on answers to the following questions:

1) Did the employer establish prior consent from employees that monitoring would take place?

   The employer would need to provide proof that the employee was informed that monitoring could in fact occur.

2) Could the employer prove that he or she had a legitimate reason for the monitoring of their employees?

   If the employer could provide justification for the monitoring in terms of a legitimate business need (e.g. the training of employees) the invasion would have a better chance of being found as legal.

3) Did the employer provide minimal intrusion; that is, did he or she cease employee monitoring immediately upon realization that the conversation was personal in nature?

   If the only calls monitored were business-related, the employer would be viewed as less invasive by the Court.

If the employer could answer "yes" to all three of the above questions, the employer's wiretap monitoring probably would be seen as legal in the eyes of the Court.

Workplace Search-and-Seizure Cases:

Just as there were similarities between our fictional E-mail case and cases involving telephone wiretapping, there are also similarities between E-mail access and workplace desk-search cases. It could be argued the electronic files of an employee really are an extension of the employee's desk. A manager searching through an employee's electronic E-mail messages is similar to a manager rummaging through an employee's desk drawer or file. The privacy issues are very much the same. Prior Court deliberations on workplace desk search and seizure cases may, as in wiretapping, provide insight into privacy interpretations of the Court. In public sector search-and-seizure cases, has it been found that an employee's privacy rights been violated? What would the courts demand from either side, employee or employer and under what condition, to prove their case? The Supreme Court consideration of *O'Connor v. Ortega* (1987) may provide some answers and some insight into E-mail privacy interpretations.

Dr. Magno Ortega had been the Chief of Professional Education at Napa State Hospital for over seventeen years. Ortega had been accused of possible improprieties and Dr. Dennis O'Connor, the Executive Director of the hospital, requested that Ortega remain off hospital premises during

investigation proceedings. At some point during the investigation, the decision was made to enter Ortega's office to search his desk and file cabinets. The reason for this search was disputed between the parties and remains unknown. Items seized included the billing files of one of Ortega's private patients and personal items such as a photograph and a Valentine's day card. All other office remnants were boxed up and stored for Ortega to reclaim (Kilburn, 1988, p. 794). This search was not influential in the decision to dismiss Ortega, but nevertheless he was eventually terminated (Rosenbloom and Carroll, 1990, p. 118). Dr. Ortega brought action against Dr. O'Connor and the hospital,[12] alleging that the search of his office and personal items violated his right to be free from unreasonable government search and seizure under the Fourth Amendment.

In order to come to a decision on *Ortega,* the United States Supreme Court had to establish two areas of guidance. First, how to best determine whether the respondent had a reasonable expectation of privacy in his work area. Second, an appropriate Fourth Amendment standard needed to be established, in order to determine the reasonableness of a government search in an area where a government employee is found to have a reasonable expectation of privacy *[O'Connor v. Ortega,* 1987, pp. 1494-1495).

In considering the first question, the Court's plurality held that the determination of a public employee's reasonable expectation of privacy must be considered on a case-by-case basis. In most other instances, it has been ruled that employees have a reasonable expectation of privacy in any personal items that they own or are of personal interest, such as a briefcase, personal mail, a desk, filing cabinet or credenza (Witt, 1992, p.555). in Ortega, the plurality relied on "undisputed evidence" in their conclusion that Dr. Ortega had a reasonable expectation of privacy in his desk and files. This evidence included the fact that Ortega did not share his desk or file cabinets with any other employees, had occupied his office for over seventeen years, had a desk and numerous cabinets which could be locked, and had an office with a locking capability. In addition, the Ortega plurality noted that "there was no evidence that the Hospital had established any reasonable regulation or policy discouraging employees ... from storing personal papers and effects in their desks or file cabinets" (*O'Connor v. Ortega,* 1987, p. 1499).

The plurality concluded that once a reasonable expectation of privacy has been established, the second area of consideration, the appropriate Fourth Amendment standard for determining the legality of the search, should be applied by balancing the employee's reasonable expectation of privacy against the government's need for supervision, control and efficiency. The need of government should be judged "by the standard of reasonableness under all the circumstances" *[O'Connor v. Ortega,* 1987, p. 1502). In reaching this conclusion, the plurality dismissed the requirement of probable cause *[O'Connor*

v. Ortega, 1987, p. 1502) and stated that a warrant is not needed for an employer's work-related search of an employee's office, desk, or file cabinets *[O'Connor v. Ortega,* 1987, p. 1500-1501).

Justice Sandra Day O'Connor provided guidelines for the standard of reasonableness which involved a two-fold inquiry: first, the search must be "justified at its inception"; second, the search must be "reasonably related in scope to the circumstances which justified the interference in the first place" (O'Connor v. Ortega, 1987, p. 1502). An office search would be justified at its inception "when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a non-investigatory work-related purpose such as to retrieve a needed file *(O'Connor v. Ortega,* 1987, p. 1502). In regard to the second part of the two-fold inquiry, the search "will be permissible in scope when 'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of ... the nature of the [misconduct]'"[13] *(O'Connor v. Ortega,* 1987, p. 1502).

For the public manager and public employee, these guidelines, in and of themselves, provide minimal guidance at best, and some have called for more clarification. For example, there has been criticism of what constitutes reasonableness.[14] However, a handful of *post-O'Connor* cases may provide additional understanding.

The establishment of an employee's reasonable expectation to privacy was discussed in the case of *Schowengert v. General Dynamics Corporation* (1987). The Ninth Court of Appeals reasoned that the plaintiff had reasonable expectation of privacy due to the lack of office practices and procedures or regulations (Wald and Kahn, 1990, p. 311). In *American Postal Workers Union v. United States Postal Service* (1989), a case which concerned the search of 1,610 employee's lockers, the Seventh Circuit Court of Appeals emphasized several factors which determined that the employees had no reasonable expectation of privacy. The factors again involved organization-established regulations authorizing searches in the workplace. Each employee had acknowledged in writing that his or her locker could be inspected at any time *[American Postal Workers Union v. United States Postal Service,* 1989, p. 560). A collective bargaining agreement had been established which authorized locker searches so long as the Postal Service had reasonable cause to suspect criminal activity or as long as a union steward was given the opportunity to be present when the search was conducted *[American Postal Workers Union v. United States Postal Service,* 1989, p. 560). The employees' argument that they had a reasonable expectation of privacy due to the fact that the Postal Service had never conducted such an extensive search in the past was rejected by the court (Wald and Kahn, 1990, p. 311).

In cases which have interpreted the second guideline, the balancing of government need against the employee expectation of privacy through a reasonableness standard, most have concerned drug testing. In *Skinner v. Railway Labor Executive's Association* (1989), *National Treasury Employees Union v. Von Raab* (1989), and *Chicago Fire Fighters Union, Local 2 v. City of Chicago* (1989), the court applied a balancing test which weighed the government's interest in public safety against the employee's privacy expectations. In these cases, the government interest in public safety was seen as more important than the employee's expectation of privacy (Wald and Kahn, 1990, p. 312).

The cases described above suggest that in a situation where a public manager opens an employee's desk, a court is likely to ask the following questions in order to assess whether the employee's rights were violated:

1) Did the employee work in an environment that afforded a "reasonable expectation" of privacy?

   In determining whether an employee has this reasonable expectation of privacy, each case must be considered individually. To determine this reasonable expectation of privacy, the courts must review the property interests of the employee, the office procedures and practices and the facts surrounding the access (Witt, 1992, p. 558).

   An employer would need to supply office environment information as proof (e.g. written regulations that searches may be conducted, work-related reasons for other employers to access the office, absence of cabinet or office locks, the number of employees in the office, etc.)

2) If the employee did enjoy a reasonable expectation of privacy, then does this expectation of privacy outweigh the government need to conduct the search?

   Generally, the Court appears to balance the employer's interest in supervision, efficiency and organizational control against the employee's interest in privacy *[O'Connor v. Ortega,* 1987). When balancing these interests, a search conducted by a supervisor for work-related purposes probably would be seen as legitimate by the Court. However, if the search is conducted solely for the purpose of obtaining criminal evidence, the employer is no longer acting as a supervisor. In cases such as these, a warrant would be necessary (Witt, 1992, p. 559).

   Finally, in cases where a public employee's performance is important to the safety of citizens, the courts have weighed heavily in favor of the employer.

If the response to both of these questions is "yes", then the Court would probably find that the rights of the employee were violated.

The Lessons Applied to the Fictional E-mail Case

What can we learn from the above cases that would apply to our fictional E-mail situation? What common logic is displayed? What common considerations are taken? How do these considerations then apply to an E-mail invasion case such as the one described in our point of departure? What rules have been established?

In order to learn from these past experiences, we must first organize the issues and considerations discussed above in some order. Table 1 supplies a summary of the above discussion. Essentially, regardless of the technology (wiretapping or simple workplace search) this analysis shows clearly that the United States courts apply a "balancing approach" when considering a workplace privacy case. This balancing approach takes into account the employee's expectation of privacy and weighs this expectation against the legitimacy of the search conducted by the employer, along with how well the employer tried to respect the employee's privacy in personal matters ("minimal intrusion"). The issues described in Table 1 should be familiar from previous discussion and will not be repeated here. One question however remains: how would these considerations be applied in an E-mail context?

TABLE 1 -- APPROXIMATELY HERE

Issue 1: Does the Employee Possess A Reasonable Expectation of Privacy in an E-mail Environment?

Most electronic mail systems store messages in files that the employee will later access, very similar to the situation where an employee accesses periodically a designated office (paper) mailbox. Usually these E-mail systems require that the employee enter a personal password, similar to a lock on an office file cabinet. The E-mail received is specifically addressed to the employee and because of the use of the personal password the employee does hold a reasonable expectation in privacy. Consequently, unless the employer informs employees that E-mail monitoring may in fact take place, the previous case law suggests that an invasion *would* violate the employee's privacy (Witt, 1992, p. 558). This is even true when considering cases where the public organization owns or provides the computer system *[Schowngerdt v. General Dynamics Corporation,* 1987, pp. 1328, 1333; Witt, 1992, p. 558).

In considering the employee's reasonable expectation of privacy in an E-mail case, Droke (1992) suggests that the court consider a number of E-mail specific factors. First, had the employer provided any notice to employees that an E-mail access may in fact occur? If so, obviously, the expectation of privacy would be reduced. Second, if no prior notification was provided, would an average employee in the organization have realized that management had the capability to access E-mail transactions? This question is applicable because in many public organizations (e.g. computer support organizations) this certainly would be the case. Public settings are becoming more and more computerized, and thus, this consideration is becoming more and more important. Third, what is the specific attributes of the E-mail system? Is there an employee-assigned password or is the password controlled by the organization (as some bank teller machine numbers are assigned by the bank). In the case where a number is assigned and maintained by the organization, an employee's expectation of privacy would be dramatically reduced (Droke, 1992, p. 185).

Issue 2: Was the Monitoring Justified?

The justification for the manager's access in our fictional case would be considered by weighing the employee's reasonable expectation of privacy against the organization's need to maintain efficiency and control (O'Connor v. Ortega, 1987). When an employer's actions are justified by a legitimate business need or to investigate employee business related misconduct, the search is seen as reasonable under Fourth Amendment constraints. Many organizations have become highly reliant on E-mail for communication between employees and even with external organizations.[15] In these situations, it is often the case that the manager of the organization must be supplied with the employee's computer password so that the manager can cover for the employee should the employee be absent. This type of action taken by an employer would most likely be seen as justified in a court of law. If however, the employer conducts the search in order to obtain evidence of criminal activity and has no warrant, the employer now has breached the allowable actions as "employer" and now wears the hat of "government investigator." Consequently, in this situation, the employee's Fourth Amendment rights would be violated (Witt, 1992, p.561).

Issue 3: Was There an Emphasis on "Minimal Intrusion" by the Employer?

Probably the most difficult of the three issues to consider is the concept of minimal intrusion. In the case of *Watkins v. Berry* (1983), the court suggested that should the employer decide to access an employee's conversation (wiretapping), it should be done with respect for the individual's privacy relating to personal discussions. As soon as the employer realizes that the communication's subject is of a personal nature, the monitoring should cease. Clearly this logic would apply to our E-mail case as

well. If the employer, in reading E-mail realizes the message is of a personal nature, the employer should not continue reading it. This concept should then cause public employers to think twice prior to taking action upon an employee based on evidence found in an E-mail transaction of a personal nature.

Limitations in the Lessons Learned:
Differences in the Physical Nature of E-mail

While there is much we have learned from the comparison of the E-mail situation, the physical differences in the technologies do pose some additional puzzles. As Ostrom (1991, p. 509) suggests, physical properties of technologies in use may dramatically influence the actions employers may have available to them. Electronic access to information has in many situations "stealth-like" properties; a manager utilizing the correct technological mechanisms could access an employee's E-mail without leaving a trace that the access occurred. This ability to keep the monitoring activity secret is reduced in non-electronic mail situations. For example, in a situation such as the one where a manager accesses an employee's desk files, the access may leave physical clues that the access was conducted. Items in the desk may be shuffled or misplaced. In addition, the manager would have to physically visit the office to conduct the search. The fear of leaving physical clues may provide a "natural" monitoring mechanism which deters many managers from taking illegal monitoring action. In the E-mail environment however, the absence of these clues may provide an environment where monitoring may be more inviting simply because the risks of being caught are reduced. These stealth-like attributes of the E-mail environment do not change the Court's considerations, but they may increase the likelihood that illegal manager access occurs.

In addition, the physical nature of E-mail may allow the organization to institute rules which may not be feasible in other technological environments. For example, in an E-mail environment, the organization may choose simply to have all employees sign a document of understanding stating that the computer system (and the use of E-mail) is for business purposes only - no personal information be stored within the system ~ thus alleviating the worry that monitoring stumbles on personal matters. In a telephone wiretapping scenario a "no personal call" policy would most likely be unacceptable, simply because one cannot cut off employees from the outside world during working hours.

Conclusion:
E-mail Privacy Guidelines For Public Organizations

New technological developments do not always result in new policy issues. From a privacy standpoint, the interception of an E-mail transaction is very much like the wiretapping of a phone conversation or the reading of memorandum kept in an office desk drawer. An employee's expectation to privacy of his or her computer files is very much like his or her privacy expectations about his or her desk or file cabinets. The analysis above supports the conclusion that there is much we can learn about how the managers in a public organization should handle an E-mail system, despite the fact that no public sector E-mail case has been deliberated in court.

The previous case analyses provide three clear privacy guidelines which public managers should apply to their E-mail environment:

E-mail Privacy Guideline 1:

Document your organization's E-mail privacy policy and communicate this to your employees.

Both wiretapping and search cases require employers to provide proof that either the employees had provided prior consent to monitoring or had been in an environment where no reasonable expectation of privacy existed. In an E-mail case, clearly the courts would ask similar questions.

An organization's policy in regard to manager access to employee E-mail should be clearly communicated to the employees of that organization. Many employees do not realize that their E-mail can be accessed by others, as was the case of Oliver North and John Poindexter when they learned that investigators had retrieved "deleted" E-mail messages concerning Iran-contra events (DeBenedictis, 1990, p. 26). In the wake of a private sector dispute over manager access to E-mail, Epson America Inc. distributed to all employees an internal memorandum warning them that they should not expect privacy in their E-mail transactions (Nash, 1990, p. 78). DePaul University College of Law's computer system provides an electronic notice to users upon access, which notifies them that "all messages shall be deemed to be readily available to the public" and privacy should not be expected (Hernandez, 1988, p. 32). Warner Brothers on the other hand, implements their E-mail policy from the opposite viewpoint: their policy states "[i]f it's not addressed to you, it's not yours" (Nash, 1990, p. 78). The point is, no matter what stance an organization takes concerning E-mail privacy, it should be clearly documented and communicated to the employees.

E-mail Privacy Guideline 2:

Be certain that your organization has a legitimate need to monitor employees' E-mail prior to **undertaking** the **action.**

In the cases discussed earlier, the courts consistently questioned the reasoning underlying managerial action. In the case of *O'Connor,* a search was undertaken which later had no influence in the eventual termination of the employee (Rosenbloom, 1990). The public manager's ability to conduct an E-mail search is dependant on the organization's privacy policy discussed in guideline one, but a privacy-conscious manager is one who clearly understands his or her actions before he or she acts. Prior to reviewing employees' E-mail without their consent, the manager must clearly consider whether the need to conduct government business outweighs the privacy expectations of the employee. Is the invasion required to satisfy a crucial business need? Is E-mail access so urgent that it cannot wait until the employee returns to the office? Is there some safety concern which is prompting a manager to read the employee's E-mail? If these questions can all be answered "no," the manager should probably refrain from taking the monitoring action.

E-mail Privacy Guideline 3:

Respect your employees' personal privacy should you **decide** to access E-mail.

Finally, the previous discussion on wiretapping highlighted the Supreme Court's concern on "minimal intrusion" - exemplified in their instructions to a lower court to determine whether the manager monitored a personal call longer than necessary (Watkins v. L. M. Berry, 1983). Even if the organization has established an "E-mail system to be used for business related purposes only" policy, employee E-mail messages may still contain personal information in messages to and from other co-workers (e.g. Westin's "emotional release" type messages). Message content becomes merky in what is defined as "personal" and what is "business related". Even with this "business purposes only" policy in place, managers still should access E-mail with the concept of minimal intrusion in mind.

Minimal intrusion may be more difficult to achieve when reading E-mail. However, there are actions a manager can take to reduce the impact of E-mail access. Many E-mail systems provide the sender with a "subject" area at the beginning of the E-mail message. Managers who do review an employee's E-mail would be wise to filter the messages using this subject area if one exists. If the subject, sender name or recipient name gives the appearance that the message is of a personal nature, the manager should read no further in regard to that message. Granted, this suggestion is limited because many E-

mail users do not use subject headings and in addition, some E-mail facilities do not provide the subject feature. But for systems that do, users can help themselves by marking "personal" in the subject of all personal messages they send. This would assist managers who monitor in doing so with minimal intrusion.

There has been much discussion recently of an "information superhighway" would allow electronic data and messages to be transmitted across the United States. The increase in the use of E-mail throughout the 1980's and early 199O's along with the importance given to improving electronic communication technologies clearly shows that the use of electronic communication will continue to increase. This increase, unfortunately, will lead to more situations like the one that took place in Colorado Springs. Armed with that realization, public managers should understand the implications of E-mail intrusion - something they may give little consideration. Public employees as well should not expect that they can simply write anything to anyone using E-mail and assume that only the addressed recipient will access the message. Simply put, all public employees would be wise to protect themselves by considering the implementation of the above guidelines for their organization.

Issue deliberated by Court	Considerations	Applicable Cases
Issue 1) Did the employee have a reasonable expectation of privacy?	Was prior consent to the monitoring given by employees? Employee's private property, locked office furniture and doors, organization search policies all contribute to this privacy expectation.	*James v. Newspaper Agency Corporation* **(1974)** *O'Connor v. Ortega* (1987) *American Postal Workers Union v. United States Postal Service* (1989) *Schowengert v. General Dynamics Corp.* (1987)
Issue 2) Was the monitoring justified?	Employer must prove that search was conducted for legitimate business purposes. Proof that the search was required to ensure public safety strongly justifies the action.	*James v. Newspaper Agency Corporation* (1974) *O'Connor v. Ortega* (1987) *Skinner v. Railway Labor Executive's Association* **(1989)** *National Treasury Employees Union v. Von Rabb* (1989) *Chicago Fire Fighters Union, Local 2 v. City of Chicago* **(1989)**
Issue 3) Was there an emphasis on "minimal intrusion" by the employer?	Employer must show that in the process of the search they respected and tried to avoid intruding upon personal items or information that may be in the office.	*Watkins v. Berry* (1983)

Table 1: Summary of Issues and Considerations of Wiretapping and Workplace Search and Seizure Cases

Notes

1. An E-mail user's computer can be connected to others in a variety of ways. The connection may connect people in a department, an organization, a continent or even the world. The simplest connection allows users to interact directly through a cable, usually within a building or buildings. Other more dispersed organizations may use a device called a "modem" which connects the user to standard telephone lines, transmitting and storing these messages in a larger "host" computer system.

The number of users in an E-mail system vary greatly from computer system to computer system and most E-mail systems do not require both parties of the communication to be accessing the system at the same time. Some electronic systems copy each message as it is transmitted, while others destroy the message after it is transmitted. Unlike telephone communication, a copy of the message (stored in archive) may survive even though the E-mail recipient deleted his or her copy of the message (Droke, 1992). This is in fact what happened to Oliver North in regard to Iran-Contra E-mail messages he thought he had deleted (Debenedictis, 1990).

2. The term "public sector" or what constitutes the public sector is under debate. Bozeman (1987) argues that all organizations have a degree of "publicness" to them. The concept of publicness to a large extent is based on revenue source. The issue of the blurring of the public and private is acknowledged but will not be addressed here. The definition of the "public sector" in this context is taken from Stillman (1987, p. 2). The public sector (what he labels "public bureaucracy") is "the structure and personnel of organizations, rooted in law, that collectively functions as the core system of U.S. government and that both determine and carry out public policies using a high degree of specialized expertise."

3. There are a number of ways a manager could intercept or access an employee's e-mail messages. In most organizations there exists some information system support organization which is responsible for the maintenance of the organization's computer system(s). It is normally chartered with ensuring that the systems stay running as well as ensuring that important files stored on the system are "backed up" in case the system has severe problems of one kind or another. Consequently, the manager could get access to the backup copies of E-mail, such as in the case of Colorado Springs, or the manager could use some authority and perhaps get access to the on-line storage of e-mail transactions. Finally, in many organizations, the manager has the authority to access an employee's computer account in the event that the employee is not available. A manager therefore could use this authority and access the employee's account and read E-mail transactions.

4. This is an interpretation from the discussion of Westin's privacy theory, presented next.

5. The term "government" in this context is defined as any person (performing the duties of his or her position) in any organization which is part of the executive, legislative or judicial apparatus of a Federal, State or Local level of governance in the United States.

6. This reasoning was set forth in *New Jersey v. TLO* (1985). In this case the Supreme Court extended the privacy rights of individuals into the workplace. They concluded that searches by government employers of the private property of employees are subject to Fourth Amendment constraints.

7. The Fourth Amendment of the United States Constitution provides individuals with the right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures..."

8. 18 U.S.C.A. sections 2510-20 (West Supp. 1982).

9. See *James v. Newspaper Agency Corporation,* 1979. Also *Simmons* v. *Southwestern Bell Telephone Company,* 1978.

10. *Watkins v. L.M. Berry & Company,* 1983 at 583.

11. See 18 U.S.C.A. section 2510 (5) (a).

12. 42 U.S.C. Section 1983 (1981).

13. The Court used reasoning developed in *New Jersey v. TLO* (1985). The case involved an assistant vice principle who conducted a search of a student's purse. The student brought action against the school for invasion of privacy under the Fourth Amendment. The Court stated that the Fourth Amendment has been held to apply to the actions of government officials in civil capacities *[New Jersey v. TLO,* 1985, p. 334-335).

14. For example, E. Miles Kilburn concludes: "the attempt to clarify the practical meaning of a 'reasonableness' standard through references to 'reasonable grounds' and 'measures reasonably related to the objectives' is redundant and adds no substance to the vacuous standard announced." (Kilburn, 1988). See also Larson (1988), page 437.

15. The Department of Defense has long used networks such as Internet to communicate, and the trend is growing. For example, organizations are beginning to use computer networks and E-mail to communicate with outside vendors in purchasing and other transactions (commonly referred to as "Electronic Data Interchange" or EDI).

References

American Enterprise Institute for Public Policy Research, 1979. *Privacy Protection Proposals.* Washington D.C.: American Enterprise Institute for Public Policy Research.

Bozeman, Barry, 1987. *All Organizations are Public: Bridging Public and Private Organization Theories.* San Francisco: Jossey-Bass.

Clucky, Laura, 1988. "The Electronic Communications Privacy Act of 1986: The Impact on Software Communications Technologies." *Software Law Journal,* vol. 2, (Spring): 243-263.

DeBenedictis, Don J., 1990. "E-mail Snoops: Reading Others' Computer Messages May Be Against the Law." *American Bar Association Journal,* vol.11 (September): 26-27.

Droke, Michael W., 1992. "Private, Legislative and Judicial Options for Clarification of Employee Rights to the Contents of Their Electronic Mail Systems." *Santa Clara Law Review,* vol. 32, no. 1: 167-198.

Duffey, Jan, Stephen P. Pepe and Beverly Gross, 1987. "Big Brother in the Workplace: Privacy Rights Versus Employer Needs." *Industrial Relations Law Journal,* vol. 9: 30-52.

Fishman, Clifford S., 1990. *Wiretapping and Eavesdropping.* Rochester: Lawyers Cooperative Publishing.

Furfaro, John F. and Maury B. Josephson, 1990. "Electronic Monitoring of Employees: Part II." *New York Law Journal,* August 6: 3.

Hernandez, Ruel T., 1988. "ECPA and Online Computer Privacy." *Federal Communications Law Journal,* vol. 41, November: pp. 17-41.

Kilburn, E. Miles, 1988. "Fourth Amendment - Work-related Searches by Government Employers Valid on 'Reasonable' Grounds." *The Journal of Criminal Law and Criminology,* vol. 78, pp. 793-827.

Larson, Keith Phillip, 1988. "Governmental Intrusion Into the Public Employee Workplace - O'Connor v. Ortega." *Creighton Law Review,* vol. 21, pp. 421-437.

McClellan, Grant S., 1976. *The Right to Privacy.* New York: The H. W. Wilson Company.

Omnibus Crime Control Act and Safe Streets Act, 1982. 18 U.S.C.A. Section 2510-20. West Supp.

Ostrom, Elinor, 1991. "A Method of Institutional Analysis and an Application to Multiorganizational Arrangements." In F. X. Kaufmann (ed.) *The Public-Sector - Challenge for Coordination and Learning.* Berlin and New York: Walter de Gruyter, 501-23.

Rohde, Stephen F., 1988. "Origins of the Right to Privacy." *Los Angeles Lawyer,* vol. 11 (March): 45-53.

Rosenbloom, David H., 1990. "What Every Public Personnel Manager Should Know About the Constitution", in S. W. Hays and R. C. Kearney (eds.). *Public Personnel Administration.* New Jersey: Prentice Hall.

Rosenbloom, David H. and James D. Carroll, 1990. *Toward Constitutional Competence: A Casebook for Public Administrators.* New Jersey: Englewood Cliffs.

Stillman, Richard J. II, 1987. *The American Bureaucracy.* Chicago: Nelson-Hall.

Wald, Martin and Jeffrey D. Kahn, 1990. "Privacy Rights of Public Employees." *The Labor Lawyer,* vol. 6 (Spring): 301-318.

Webster's Ninth New Collegiate Dictionary (Springfield: G. & C. Merriam Company), 1988.

Westin, Alan F., 1967. *Privacy and Freedom.* New York: Atheneum.

Witt, Lois R., 1992. "Terminally Nosy: Are Employers Free To Access Our Electronic Mail?" *Dickinson Law Review,* vol. 96, no. 3: 545-571.

Court Cases

American Postal Workers Union v. United States Postal Service, 1989. 871 F.2d 556 (6th Cir)

Chicago Fire Fighters Union, Local 2 v. City of Chicago, 1989. 717 F. Supp 1314

Grizwold v. Connecticut, 1965. 381 U.S. 479

James v. Newspaper Agency Corporation, 1979. 591 F.2d 579

National Treasury Employees Union v. Von Raab, 1989. 109 S. Ct. 1384

New Jersey v. TLO, 1985. 469 U.S. 325

O'Connor v. Ortega, 1981. 42 U.S.C. 1983

O'Connor v. Ortega, 1987. 107 S. Ct. 1492

Olmstead v. United States, 1928. 227 U.S. 438

Schowengert v. General Dynamics Corporation, 1987. 823 F.2d 1328 (9th Cir)

Simmons v. Southwestern Bell Telephone Company, 1978. 452 F Supp 392

Skinner v. Railway Labor Executive's Association, 1989. 109 S. Ct. 1402