January 1994

UILU-ENG-94-2202
ACT-130

Applied Computation Theory

ETHICS AND THE PRIVACY OF ELECTRONIC MAIL

Erini Doss

Coordinated Science Laboratory
College of Engineering
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

Ethics and the Privacy of Electronic Mail

Erini Doss

Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
Urbana, Illinois 61801

January 1994

1. Introduction

Electronic mail (e-mail) is a relatively new form of communication. There has been no previous scholarly investigation of the ethics of e-mail, however. In this paper, I shall outline current legal protections for e-mail privacy, and explain how e-mail is treated in corporations and universities. I shall conclude with why I believe it should be private in **all** environments.

1.1 Advantages of e-mail

Electronic mail is a popular method of communication today. In the United States alone, more than 19 million e-mail users send and receive 15 billion messages a year (Rothfeder, 1993). Why do some people prefer e-mail over telephones and fax machines? First, electronic mail is inexpensive. For example, a one-page e-mail message sent from California to New York costs only about 16 cents, compared with $1.86 if sent by fax, and $13 if sent via overnight express mail (Rothfeder, 1993). Another advantage of e-mail is that information can be exchanged quickly. As a result, it is a valuable tool for businesses because it improves responsiveness between managers and employees. For example, if managers want to communicate something to their fellow employees, they no longer have to call them and leave

messages on their answering machines. Instead, managers can send co-workers e-mail messages that will reach their computers, regardless of whether they are sitting at their computers at that moment. Managers then also avoid making telephone calls at late hours; they can simply e-mail their thoughts to their employees. Individual electronic mail users also benefit because they no longer have to waste time playing telephone tag or worry about having to communicate with others only during strict business hours.

1.2 Disadvantages of e-mail

E-mail also may have disadvantages for users, however, because e-mail may not be considered private. E-mail messages can be saved on magnetic tape and be used in a court of law. Although telephone conversations and postal letters are not admissible in court without permission of both parties involved, e-mail can be used as evidence in court. This difference exists because fundamentally, e-mail is not necessarily treated as private, whereas phone conversations and letters are. In the seminal e-mail case, *United States vs. Poindexter,* a federal judge ruled that e-mail sent by John Poindexter to Oliver North could be used as evidence in court against Poindexter, if it explicitly told of illegal activities (Eskow, 1993). Electronic mail between police officers was introduced by the prosecution in the Rodney King trial in Los Angeles. In this case, several white police

officers were accused of misconduct when they stopped a black man, Rodney King, on the highway and attempted to arrest him. King fought back as they tried to handcuff him. An eyewitness captured some of the scene on videotape. The tape showed that even after King stopped retaliating, the police officers continued to hit him. The e-mail exchanged between these police officers afterwards confirmed their cruel treatment of King (Mnemonic, 1993).

2. Questions Concerning E-mail Privacy

Following the Poindexter and King cases, many questions concerning privacy rights for e-mail have been posed to the federal and state courts:

Is there a clear definition of privacy?

Why is privacy so important to people?

Should privacy be viewed by the courts as one of the rights that is protected by the Constitution?

If the courts define a standard of privacy that can not be broken except under extenuating circumstances, can it apply to e-mail?

Should e-mail, like other forms of communication such as postal letters and telephone conversations, be treated as private?

Should e-mail be treated as private in some settings and not in others?

I will answer these questions from both philosophical and legal standpoints. Warren and Brandeis, Rachels, and other philosophers and lawyers have attempted to define privacy. Unfortunately, there is still no clear, widely accepted definition of privacy. Consequently, it is difficult to determine privacy rights should be absolute. Today, privacy rights differ according to users' settings. For example, corporate and academic treatments of e-mail are different. It seems reasonable to hypothesize that the reason for the difference is economic: academics don't have trade secrets. I will conclude this paper by arguing why I believe e-mail should be absolutely private in all settings, for ethical reasons. Regardless of whether privacy is Constitutionally protected, it remains with a person in all settings except when breached for legitimate reasons. Thus, e-mail should not be treated as private in some settings and not in others.

3. Definitions of Privacy

3.1 Philosophical Definitions

Before I can reasonably determine whether e-mail should be private, I need to define privacy. In the classic paper on privacy, Warren and Brandeis assert that privacy is the

right to be left alone (Warren and Brandeis, 1890). They believe that privacy ends when facts about another individual are made known to the public. I will illustrate this concept using two fictional characters, Alice and Bob. For example, if Alice **chooses** to disclose information to Bob, her privacy ends. Warren and Brandeis argue that the right to privacy means that people have the right to keep others from obtaining personal information about them.

In the decision of *Eisenstadt vs. Baird,* privacy is defined as the "the ability to exert control over information pertaining to our own lives" (*Eisenstadt vs. Baird,* 1972). Unlike the definitions of Warren and Brandeis, this definition does not imply that if Alice chooses to disclose personal information to Bob, then she loses her privacy (Parent, 1983). Instead, the court's definition implies that Alice's privacy is invaded only if she does not have the ability to control that personal information. For example, if Alice's past criminal record is exposed by Bob without her permission, then her privacy has been taken away. Should her criminal past be disclosed to a potential employer, for example, she will most probably not be offered a position. Thus, her past is controlling her future. I feel that the *Eisenstadt vs. Baird* definition of privacy is the most practical because it takes into account freedom of choice. If Alice tells Bob of her past drug abuse in confidence, and Bob does not tell anyone else, then Alice has not given up her privacy. Only if Bob breaks his vow of secrecy to her

and tells others such as Cindy, David, and Erin will Alice's privacy be invaded.

3.2 Legal Definitions

Federal and state courts have attempted to define privacy. For example, in *Long Beach City Employees Association vs. City of Long Beach,* the judge stated,

> The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion and our freedom to associate with the people we choose (California Supreme Court, 1986).

This is similar to Warren and Brandeis's definition of privacy.

In *Wilkinson vs. Times Mirror Corporation,* the judge said,

> The general concept of privacy can be viewed as encompassing a broad range of personal action and belief. However, that right, much as any other constitutional right, is not absolute. A court

> must engage in a balancing of interests rather than a deduction from principle to determine its boundaries. Stated another way, a court should not play the trump card of unconstitutionality to protect absolutely every assertion of individual privacy (California Court of Appeals, 1989).

In this decision, the judge explored the limitations of privacy.

3.3 Why is privacy so important?

People value privacy because it allows them to share personal information only with whomever they choose. Suppose that Erin tells Frank that she served a jail sentence in the past, and Frank tells her employer. After knowing this fact, her employer may treat her differently. For example, he may monitor her work more carefully because he does not trust her. Consequently, Erin will be more careful in the future about revealing herself. Suppose Erin does not tell Frank about her past jail term, but he hears about it from someone else. Frank now has power over Erin that she has not granted him. He has the ability to hurt Erin with the information he has about her. If Frank dislikes Erin, he may tell her fiancé and business associates of her past. Erin's fiancé may cancel the wedding because he feels that Erin has not been totally honest with him. Her business associates may

not respect and trust her as much as they used to. Thus, Erin may be put in a position where she has to prove herself all over again to her fiancé and colleagues unnecessarily. Therefore, Erin's privacy has been invaded.

According to Rachels,

> The value of privacy is based on the idea that there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people (Rachels, 1984).

Privacy is important because it allows people to maintain a variety of social relationships with others. For example, Ignatius may have an intimate relationship with his wife Jill. He may tell her everything from what happens daily at work to what his views are on religion. In contrast, Ignatius has a more business-like relationship with his coworkers. He is not inclined to tell his fellow employees that he and his wife are having marital problems. Because Ignatius's relationships with Jill and his coworkers are different, he behaves differently in each. He chooses to let his wife see all of his facades. On the other hand, he never allows his fellow employees to see him lose his temper or behave irrationally.

Privacy is also important in competitive situations (Schoeman, 1984). If a renown ice-skater exposes all the

jumps and spins in her upcoming competition, she will be giving competitors a chance to copy some of her ideas. Her routine may no longer be as original as she planned. Other ice-skaters may attempt to perform even harder ice-skating routines, so that they can capture first place.

People do not like to feel that they lack control over who knows what about them. For this reason, privacy should be viewed as another inalienable right that can be violated only when it is morally justifiable to do so. Unless extenuating circumstances exist, privacy must be maintained because it can never be taken back. Once some information is made public, it can no longer be made private again. Thus, a presumption of privacy is reasonable.

4. Legal Protection for E-mail Privacy

4.1 Why there is much confusion

Why are there so many unanswered questions concerning the privacy rights of electronic mail users? Although the First and Fourth Amendments of the U.S. Constitution protect the written or printed word, electronic, unprinted "papers" are not specifically protected. According to the Fourth Amendment,

> The right of the people to be secure in their persons, houses, and effects, against unreasonable searches and seizures, shall not be violated and no warrants shall be issued without probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Thus, according to the amendment, a person's belongings or "effects," such as written papers, are safe from unreasonable search and seizure. In strict interpretations of the Constitution, since electronic "papers" are unprinted, they are not protected. As a result, one has to go beyond the Constitution to understand e-mail privacy rights.

4.2 Federal and state laws

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA). In addition to expanding the kinds of communication covered by federal privacy law, the ECPA takes a crucial step of protecting e-mail messages not only during their transmission, but during their storage in the computer as well. In other words, e-mail messages that have already been sent, received, and saved are protected from unauthorized snooping.

> The ECPA has two essential purposes: 1) to protect all electronic communication systems, including purely internal electronic mail systems and public systems, from outside intruders; and 2) to protect the privacy of certain messages sent over public service electronic mail systems just as the privacy of telephone calls over public telephone systems is protected (Podesta and Sher, 1987).

Penalties for violation of the ECPA can be harsh. The illegal interception of e-mail and the use of illegally intercepted e-mail are considered a felonies. They are punishable by a five year prison sentence and a fine (18 U.S.C.A. Sections 2511(4)). Individual violators may be fined up to $250,000, and businesses may be fined up to $500,000.

Federal law provides a minimum standard on e-mail privacy, leaving the states free to legislate further protections. California, for example, has passed extensive privacy rights laws, in addition to adding a section in its constitution about privacy rights. In the ruling in *White vs. Davis,*

> In November 1972, the voters of California specifically amended article 1, section 1 of our state Constitution to include among the various inalienable rights of all people the right of

> privacy. The moving force behind the new constitutional provision was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society (*White vs. Davis*, California Supreme Court, 1975).

According to *Wilkinson vs. Times Mirror Corporation*,

> Common experience with the increasing use of computers in contemporary society confirms that (article 1, section 1) of the California Constitution was needed and intended to safeguard individuals' privacy from intrusion by both private and governmental action. That common experience makes it only too evident that personal privacy is threatened by the information-gathering capabilities and activities not just of the government, but of private business as well (*Wilkinson vs. Times Mirror Corp.*, California Court of Appeals, 1989).

Statutory penalties for violating California privacy laws are more favorable to successful plaintiffs than those provided by ECPA (Veeder, 1993). California penalizes a range of computer-related activities, including "knowingly and without permission accessing or causing to be accessed by any

computer, computer system, or computer network" (Cal. Penal Code Section 502 (c)71). Thus, California law protects individuals, financial institutions, governmental agencies, and others within the state, who lawfully use computers, computer systems, and computer data (Cal. Penal Code Section 502(a)).

5. E-mail in Corporations

Federal and state laws protect e-mail privacy only in public networks. For example, the ECPA (federal law) does not protect e-mail privacy in private networks. Governments generally allow private companies and private networks to formulate their own policies on e-mail privacy. Policies can be imposed on employees as long as they do not contradict federal or state laws. Until recently, there was no case law on privacy in the workplace. In the few cases that have been tried, the courts have generally favored the employers except in cases where the employee has a reasonable expectation of privacy. "Reasonable expectation" is based on what a judge believes a reasonable man would do or expect in a given situation. But, what is considered reasonable? What may seem reasonable for one person may seem unreasonable to another.

Companies are adopting e-mail policies that make it clear to employees that company computers are for business use only, hence anything transmitted through them is not

private. Private corporations feel that these policies are necessary because they must protect the information in their computer systems in order to compete in the market.

Most companies, such as Digital Equipment Corporation, treat employees' e-mail as company property. From a company's viewpoint, since the company owns its computers, disks, and networks, whatever happens on them belongs to the company (Ables, 1993). Computers, like desks, paper files, notebooks, etc., are company assets provided to employees to assist them in performing their work (Digital Equipment Corporation policies handbook, 1993). These tools, and any work product they contain, are company property. Since a company's primary concern is making profit, trade secrets need to be protected. Thus, e-mail is not for private use and is subject to investigation at all times.

A company may not want its employees to use e-mail for personal purposes since e-mail overuse may prevent them from performing their work efficiently. By the same logic, shouldn't postal mail and telephone calls be monitored as well, since they too, may distract an employee? Although some companies record all phone calls and have policies saying that they can check an employee's disk anytime, these are not general practices adopted by most (Kadie, 1993). Even though managers at Apple Computers, for example, do listen in on employees' conversations, most companies do not monitor phone calls (Howland, 1993).

Then why do corporations treat e-mail differently from postal mail or telephone calls? There are two reasons: first, it is easier to monitor e-mail than postal mail or telephone calls; second, there are no established social conventions with e-mail. To read an employee's postal mail, an employer has to go into the worker's office, unlock the desk, and rummage through its contents. This can be a difficult task. Telephone calls are simply hard to tap. Compared with both postal mail and telephone calls, e-mail is easier to monitor, and e-mail can be read from the privacy of one's own office. Further, there are social rules concerning postal mail and telephone conversations: people have been taught from early childhood that it is rude to read postal mail that is not addressed to them or to eavesdrop on telephone conversations. Because e-mail is a new technology, it doesn't have such social rules.

Many corporations such as IBM, Rockwell International, and Motorola have strict policies against using company assets for personal use (Sidaris, 1993; Mitchell, 1993). Thus, writing personal e-mail is disallowed by those policies. IBM, Rockwell International, and Motorola assume that there is a clear distinction between employees' work and personal lives. These companies do not consider that employees' careers and private lives sometimes intermingle. Thus, is it logical for companies to expect that e-mail should be used only for business reasons? In the decision in

O'Connor vs. Ortega, the relationship between work and private life are investigated:

> The reality of work in modern times, whether done by public or private employees, reveals why a public employee's expectation of privacy in the workplace should be carefully safeguarded and not lightly set aside. It is, unfortunately, all too true that the workplace has become another home for most working Americans. Many employees spend the better part of their days and much of their evenings at work. Consequently, an employee's private life must intersect with the workplace, for example, when the employee takes advantage of work or lunch breaks to make personal telephone calls, to attend to personal business, or to receive personal visitors in the office. As a result, the distinctions between the workplace and professional affairs, on the one hand, and personal possessions and private activities, on the other, do not exist in reality.

Therefore, even if a company believes that it is ethical to monitor employees' e-mail, it may not be logical to do so because work and private life many times coincide.

6. Recent Court Cases

Because the ECPA does not apply to private networks, the privacy of e-mail in corporate networks may not be legally protected. Some companies feel that they do have the right to monitor e-mail, but do not make this policy known to their employees. Consequently, some lawsuits have been filed by employees. In the case of *Shoars vs. Epson,* Epson employee Alana Shoars found her manager, Robert Hillseth, printing out all employee e-mail one day. She objected and told Hillseth that his actions were unethical. A few weeks later, she was fired for insubordination. Shoars claimed that she was fired because of an e-mail message that she had sent to a colleague in which she called Hillseth a "bonehead tyrant." Shoars had assumed that her e-mail was private because she was never told that company e-mail was subject to monitoring. Ironically, she was the system e-mail administrator for Epson. Shoars brought a class-action suit against Epson for invasion of privacy under section 631 of the California Penal Code. The California Superior Court ruled that section 631, a law that forbids the interception of communications without the consent of all parties involved, did not apply to electronic mail. Shoars filed an appeal, and the case has not yet been resolved (Veeder, 1993).

In the case of *Bourke vs. Nissan,* Bonita Bourke and Rhonda Hall, two former Nissan information specialists, were criticized in 1990 by management for using Nissan's e-mail system to receive personal messages. Management handed them

a stack of printouts of their private e-mail, even though Nissan management had earlier told employees that confidential passwords protected their e-mail from interception. As a result, Hall filed a complaint with Nissan's human resources department. Nissan fired Hall a few days later. Bourke later filed a lawsuit in the Los Angeles Superior Court claiming invasion of privacy and wrongful termination of employment (Veeder, 1993).

Unlike the *Epson* and *Nissan* cases, the case of *Steven Jackson Games vs. Secret Service* involved federal law rather than state law. Steven Jackson Games is a small, privately owned adventure game maker located in Austin, Texas. One of the company's most recent products is GURPS CYBERPUNK, a science fiction role-playing game set in a high-tech world of the future. The U.S. Government became suspicious of Steven Jackson Games merely because one of the programmers of GURPS CYBERPUNK was a former computer hacker. As a result, On March 1, 1990, just weeks before the release of GURPS CYBERPUNK, Secret Service agents raided the premises of Steven Jackson Games. The Secret Service agents seized three computers, including the one that was used to design the new game. They also took all the company software located next to the computers taken, the company records located on these computers, and whatever they could find in the company's warehouse. All working drafts of the game book both on disk and paper were confiscated because the Secret Service believed that they were handbooks for computer crime. As a

result, Steven Jackson Games filed a lawsuit claiming invasion of privacy. In March 1993, Steven Jackson Games won its case against the Secret Service and the U.S. Government. The court awarded each plaintiff $1,000 and paid for attorney's fees.

7. E-mail in Academe

Privacy tends to receive a higher priority in an academic environment than in a corporate one. Few university employees make a habit of reading the e-mail of other students, faculty, and staff (Kadie, 1993). While some incidents of breaches of privacy do occur, they are usually for legitimate reasons. For example, if a student is accused of murder, the prosecutor may obtain copies of the student's mail. At the University of Illinois at Urbana-Champaign, the Interim E-mail and Computer File Privacy policy says that "networks and system administrators are expected to treat the contents of electronic files as private and confidential." Similar policies exist at the University of Michigan and at Washington University in St. Louis. At the University of Michigan, "the University characterizes as unethical any activity through which an individual without authorization invades the privacy of individuals or entities that are creators, authors, users, or subjects of the information resources" (The Electronic Frontier Foundation, 1993). The

policy at the Washington University Center for Engineering Computing is similar:

> All user [e-mail] accounts are considered the private domain of the user who owns them. All users should expect that, regardless of the protections set on their files, they will not be read by others. System Management will only view users' files under exceptional circumstances (The Electronic Frontier Foundation, 1993).

Why do universities treat e-mail as private and companies do not? In most cases, university e-mail accounts exist so that faculty and students can communicate with one another and with those at other universities. They use e-mail for both academic and social reasons. In contrast, e-mail facilities in corporations exist to maintain company viability and profitability. Also, universities have no trade secrets. For example, a graduate student may choose to publish his thesis because it belongs to him, and the publication of the thesis does not harm the university. On the other hand, in a company, all work done during regular business hours is considered to belong to the company.

Since many universities are state institutions, they must respect the Fourth Amendment's "reasonable search provisions" (Kadie, 1993). Privacy is consistent with

academic freedom. E-mail is a form of speech. All speech is protected by the doctrine of academic freedom. An official statement of the American Association of University Professors says, "On a campus that is free and open, no idea can be banned or forbidden. No viewpoint or message may be deemed so hateful or disturbing that it may not be expressed."

An excerpt from the American civil Liberties Union (ACLU) Handbook states that "there must be a reasonable suspicion directed specifically at each student before a school official can search students" (Electronic Frontier Foundation, 1993). Monitoring a student's e-mail is considered searching that student. Furthermore, the Buckley Amendment says that most information about a student cannot be disclosed to outsiders (Rothfeder, 1993). Thus, a student's e-mail can not be revealed to others in or out of the academic setting without permission. Unfortunately, there is no counterpart of the Buckley Amendment for corporate employees.

Universities exist mainly to educate students and to conduct research. Research is done with the intention of meeting the public's needs. Universities eventually make their results known to the public. The competition between universities over research money differs from competition between corporations. Often, the reputation of a university is based on the amount of beneficial research it performs. As the reputation of a university increases, brighter

students and professors flock to it. The extra knowledge and better instruction and research that students get from this reputable university may help them in the future when seeking employment. I feel that many students and professors would remain at the university without better chances of employment. Less reputable universities may make it easier for these students to graduate and professors to obtain tenure. Those who are in the academic environment primarily for knowledge however, may find those environments not satisfying. Thus, universities exist first for research, reputation, and instruction. Because research is the first goal of a university, communication between faculty and students at other universities is encouraged. Such communication may not be as frequent if professors and students know that their e-mail is not private. Less communication is detrimental to research and ultimately, to the public.

8. Why All E-mail Should be Private

Why should all e-mail be considered private? If a coworker were to see some postal letters addressed to me on my desk, he would not think to pick them up and read them. He has been taught by social conventions that to read my letters without permission is nosy. By the same reasoning, since e-mail is simply information that is stored on the

computer and transmitted between networks, it should be given the same respect as the postal letters on my desk. In the same way that it would be a breach of privacy to read my postal letters without my permission, it would be a breach of privacy for a coworker to read my electronic mail without permission. That coworker does not have the right to use his computer to examine what is in my computer. An employer, for that matter, also does not have the right to examine the contents of my e-mail.

In the same sense that a letter carrier should not give my mail to someone else and a telephone operator overhearing my call should not tell anyone else what it was about, a system operator should not disclose my e-mail to anyone other than the intended recipient. This includes managers and coworkers in a job setting, and professors and other students in an academic setting. Thus, if there is no policy about e-mail in a person's work or academic setting, he should be able to assume that it is private.

But what about companies that tell employees that their e-mail may be monitored? I still claim that monitoring of anyone's electronic mail, unless for specific extenuating reasons, is not ethical. Those companies should not monitor their employees' e-mail for business reasons, if not for moral reasons. When a branch of Hewlett-Packard announced that its managers may monitor workers' electronic mail, there was an immediate two-thirds drop in e-mail use. Some of this drop included company business matters (Rothfeder, 1993). A

company is less productive when it monitors e-mail because its employees may be paranoid about using e-mail at all, and thus, they communicate less with coworkers even about business matters. Companies that monitor e-mail may even discover that employee loyalty decreases. Employees tend to not be as loyal when they feel that they are not trusted. "Employees have to feel that you trust them, and that you are not looking over their shoulders" (Rothfeder, 1993).

Although technically it may be immoral and actually counterproductive for companies to monitor e-mail, many of them do so today. E-mail will continue to be monitored until new laws forbid the practice. As a result, employees need to be realistic and act prudently: When a company gives an employee a handbook explaining its rules on e-mail, it would be wise for that person to follow them. Generally, in a court of law, judges tend to side with the companies when an employee has broken rules that have been explicitly stated in a handbook. Thus, in the courts, whether the company has the moral right to monitor an individual's e-mail is not even an issue. What is debated is whether that person was well-informed about the monitoring. Consequently, companies today are publicizing their policies about the privacy or non-privacy of e-mail vigorously. Managers present the company's e-mail policies to workers in various ways. Policies are explained to employees in a form they sign upon hiring, in articles in employee newsletters, in computer screens when they log-in to their company computers, etc.

9. Breaches of Privacy

Breaches of privacy do occur even without ethical reasons. Suppose that a manager of Widget Engineering feels that an employee, Gigi, is not getting her work done efficiently. The manager may choose to monitor her e-mail to find the causes of her inefficiency. Her lack of motivation is not something that is punishable by law. I feel that since her inefficiency does not infringe on any laws, it is not ethical to read her e-mail. Rather than infringe on Gigi's privacy, her manager should speak to her and ask if she needs any guidance.

There are some morally justifiable reasons for a breach of privacy. For example, if Widget Engineering has reasonable suspicion that one of its workers is exchanging trade secrets with American Central Communications Inc., then Widget has the right to monitor that individual's e-mail. However, Widget Engineering must have good reason to question that person's integrity. Only then can reading that worker's e-mail be morally justifiable.

10. Guidelines for Breaches of Privacy

Even though reading someone's e-mail may be morally justifiable in some situations, specific guidelines should ensure that the privacy of that individual is respected. This logic is explained well by the California Court of

Appeals in *Luck vs. Southern Pacific Transportation Company:* "The constitutional right to privacy does not prohibit all incursion into individual privacy, but provides that any such intervention must be justified by a compelling interest" (*Luck vs. Southern Pacific Transportation Company,* 1990). The restrictions that apply to search warrants in the Fourth Amendment should also apply to reading an individual's e-mail. According to the Fourth Amendment, in order for law enforcers to obtain a search warrant, there must be a "probable cause" that criminal evidence will be at the site of the search. The Fourth Amendment also specifies that law enforcers should know exactly what they are looking for and seek only those items pertaining to that end. For example, a police officer may not walk into an office looking for a specific document and scan all information on computer disks as well. If law enforcers do find that illegal actions are being committed, then they have the right to seize only those objects that can be used as evidence. Once again, law enforcers can not go into offices, find documents that they are looking for, and grab both them and all computer software as well. These same guidelines should also apply to e-mail monitoring, since exposing an individual's e-mail is equivalent to searching that person and his belongings.

In *Steven Jackson Games vs. Secret Service,* these guidelines for breaches of privacy were disregarded. According to the Fourth Amendment, Secret Service agents may enter Steven Jackson Games only if there is probable cause

that criminal evidence will be at the site. The Secret Service decided to raid Steven Jackson Games just because one of the programmers of its newest games was a former hacker. The courts decided that there was no proof of criminal activity. The Fourth Amendment also states that law enforcers must know exactly what they are looking for and search only those items pertaining to that end. The Secret Service agents, however, seized three computers, company records, and company software. The agents wanted to search everything because they were not sure what the crime was yet. If Secret Service agents found that illegal actions were being committed, then they had the right to take only those objects that could be used as evidence. But the Secret Service agents took everything with them, including copies of the game's handbook. Ironically, there was no illegal activity at Steven Jackson Games.

11. Conclusion

U.S. citizens are entitled to the traditional rights to life, liberty, and pursuit of happiness, regardless of where they live. Privacy should be accepted as another inalienable right. It is something that is sacred to people. Electronic mail should be as private as telephone conversations and postal letters.

Currently, electronic mail privacy is treated differently in corporations and in universities. This

difference seems illogical since privacy rights should not be violated, except in extenuating circumstances. Only in the case of illegal conduct can those rights be violated. Thus, different settings should not result in different treatments of privacy.

The routine monitoring of e-mail by private corporations, without a reasonable suspicion of illegal activity, is tantamount to unreasonable search and seizure. The Fourth Amendment protects individuals against such injustices.

Since the Constitution was written when there were no computers or electronic communication, special provisions have not been made to include e-mail. However, this may change. Laurence Tribe, a Harvard Law School professor, recently proposed an amendment to the U.S. Constitution that would protect people using new technology against unreasonable search and seizure (Rothfeder, 1993). Such an amendment would probably apply to both academic and corporate environments. Consequently, Americans might no longer have to worry about losing their privacy rights when they graduate from a university and join a corporation.

Acknowledgments: I would like to thank Professor Michael Loui of the University of Illinois at Urbana-Champaign for his helpful knowledge and guidance in writing this paper. I would also like to thank David Lemson and John Fultz, two classmates of mine, in Professor Loui's engineering ethics class, for valuable information.

References

Ables, King, Electronic Foundation Frontier, 1993.

Digital Equipment Corporation Policies Handbook, 1993.

Douglas, William, *The Rights of the People* (Westport, CT: Greenwood Press, 1958).

Eisenstadt vs. Baird, 405 U.S. 438 (1972): 453.

Electronic Frontier Foundation Organization, 1990.

Eskow, Dennis, "Your E-mail Can be Used Against You, " Corporate Computing(January 7, 1993), p. 171.

Fultz, John, "Who's Reading My Mail?" May, 1993, pp. 1-3.

Howland, NASA, private e-mail message, 1993.

Kadie, Carl, Electronic Foundation Frontier, 1993.

Lemson, David, "Privacy and the Multiuser Computer System Administrator," May, 1993, pp. 3-5.

Long Beach City Employees vs. City of Long Beach, California Supreme Court, 1986.

Loui, Michael, Professor of Electrical Engineering at the University of Illinois at Urbana-Champaign, 1993.

Luck vs. Southern Pacific Transportation Company, California Court of Appeal, 1990.

Mitchell, Bill, Motorola, private e-mail message, May 9, 1993.

Mnemonic, University of Texas at Austin Unix Society, 1993.

Olmstead vs. U.S. 277 U.S. 438 (1928): 475-6.

Parent, W.A., Privacy, morality, and the law, *Philosophy and Public Affairs,* vol. 12, no. 4, pp. 269-288, Fall 1983.

Paul, Craig, Network Security Operator at Kansas University, 1993.

Podesta, John, and Sher, Michael, "Protecting Electronic Messaging: A Guide to the Electronic Communications Act of 1986." 1987,p. 8.

Rachels, J., Why Privacy is Important, in Schoeman, Ferdinand D., ed., Philosophical Dimensions of Privacy, New York, New York, 1984, pp. 353-385.

Rothfeder, Jeffrey, "E-Mail Snooping," Corporate Computing(January 7, 1993), p.168.

Savage, J.A., "E-Mail Bust Generates Privacy Rights Uproar," Computerworld(January 23, 1989), 23:2.

Schoeman, Ferdinand D., ed., Philosophical Dimensions of Privacy, New York, New York, 1984.

Schwartz, John, "How Did They Get My Name?" Newsweek(June 3, 1991), p.40.

Sidaris, Jim, Thomas Bros. Maps, 1993.

Time vs. Hill, 385 U.S. 374 (1967): 412.

Veeder, Susan B., "Electronic Mail Privacy," NCSA Conference in Washington D.C., June, 1993.

Warren, Samuel, and Brandeis, Louis, "The Right to Privacy, " *The Harvard Law Review,* 4 (1890): 205-222.

Whalen vs. Roe, 429 U.S. 589 (1977): 608.

White vs. Davis, California Supreme Court, 1975.

Wilkinson vs. Times Mirror Corporation, California Court of Appeals, 1989.