March 31, 1997

Caught in the Web: Privacy and the Internet

John Wong
University of Colorado at Boulder
Department of Sociology
Honor's Thesis

Acknowledgments

There have been numerous people who have helped me with this research project. I would like to first thank Margaret Fan for giving me constant support throughout this endeavor. Tom Mayer for accepting me into the Honor's program and giving me invaluable advice on my thesis. Gary Marx for taking a chance on me by becoming my advisor. Your expertise and knowledge allowed me to see things differently. Ed Rivers for giving excellent advice on my writing. Mary Virnoche for helping me throughout this project. I do not know if I would have completed it without your help. Richard Leo for adding on extra responsibility. Karen Vlosky for being Karen. Michael Miller and Tyler Jacobs for providing technical support. And I would like to thank the people I interviewed, the professors that allowed me to survey their classes, and the students who participated in my survey.

Table of Contents

1. Introduction 1

2. Privacy and the Internet 4
   2.1. Theoretical Models 4
   2.2. Privacy and Technology 5
   2.3. Internet Privacy 6
   2.4. E-Mail Surveillance 7

3. Methods 8
   3.1. Interviews 8
   3.2. Surveys 10
   3.3. Data Analysis 11
   3.4. Limitations 11

4. Constructing Privacy 12
   4.1. Laws 12
   4.2. Institutional Policies 15
   4.3. Normative Behavior 17
   4.4. “Anonymity is part of the Magic” 18
   4.5. Awareness of Privacy 20

5. Technological Breaches of Privacy 23
   5.1. Electronic Mail 23
   5.2. World Wide Web 27
   5.3. Unix Commands 31

6. Reasons and Justifications to Breach Privacy 35
   6.1. Fun & Challenge 36
   6.2. Boredom & Curiosity 36
   6.3. Duty & Responsibility 37
   6.4. Technological Superiority 38
   6.5. Accident 38
   6.6. Interpretations of Policies and Laws 39
   6.7. Profit 39

7. Protecting Privacy 41
   7.1. Public Awareness 41
   7.2. Gross National Privacy Invasion 41
   7.3. Code of Ethics 42
   7.4. Technologies 42
   7.5. Legislation 44

8. Conclusion 46

9. Appendix A1

10. Bibliography B1

ABSTRACT

This research examines the different ways in which Internet privacy can be established, violated, and protected. This work addresses federal and state legislation related to Internet privacy, but focuses primarily on institutional policy and cultural norms at the University of Colorado at Boulder. Moreover, this research explores the perspectives and experiences of system administrators and students at this institution. Internet privacy breaches occur because of reasons ranging from hackers searching for fun to system administrators reading people's e-mail messages. The ease in which information can be gathered on the Internet is both it's greatest strength and weakness. Having complete anonymity can lead to irresponsible behavior and having too much information gathered about a user can be detrimental to that person's identity and privacy. Therefore, law and policy makers need to be cautious in granting too much privacy; but, privacy rights should be expanded from what they are now.

1. INTRODUCTION

Supervisor	Why were you in the computer lab at 3 in the morning?
Lab Attendant	How did you know that?
Supervisor	Answer the question.
Lab Attendant	Did I set off the alarm?
Supervisor	No, just answer the question.
Lab Attendant	I couldn't sleep, so I went to lab to get some stuff done.
Supervisor	Oh.
Lab Attendant	So, how did you know?
Supervisor	I have my ways…

I have my ways of tracking people on the Internet. It's not that hard. If I wanted to see where and when a person has logged in, I type in a command. If I wanted to see what people have done lately on their electronic mail (e-mail) account, I type in a command. The Internet is a reminder of Orwell's 1984, where "Big Brother" may be watching, listening, observing.

The focus of this paper is to understand privacy on the Internet. How is privacy established and broken? Do people who use e-mail fear that their privacy is invaded? Can information be gathered about a "surfer" of the World Wide Web? Do people care if their messages are read by a third party to whom they were not sent? And if people do care about their privacy, what can be done to ensure that private information does not fall into the wrong hands?

Since 1992, the Internet has become a booming technology that seems to have permeated everywhere. Over 33 million people use the Internet and there are over 27,000 web sites. (www.anamorph.com - February 1, 1997) Most of the big

---

Author's Note: This research was supported by the Undergraduate Research Opportunities Program Grant at the University of Colorado at Boulder.

corporations have a web site; more and more people are using e-mail to communicate; small on-line communities are forming with the use of chat rooms; and all of this appears to be just the beginning.

The Internet has a lot of promise; but, it also has problems. Hackers invade people's privacy, steal intellectual property, and bring down systems used by thousands of people. For example, many financial analysts believed that Kevin Mitnick stole millions of industry trade secrets from telephone companies. (Markoff, 1995) Mysteriously, the judge and prosecutor who first sent Mitnick to jail lost everything in their savings. (Littman, 1996)

Policies and laws seem to lag behind the technology. Since 1993, the Clinton Administration has supported the approval of the "Clipper Chip."

> …the administration (Clinton) has been trying to persuade the public to support an approach to protecting the privacy of computer and telephone communications that would permit law-enforcement and intelligence-agency officials to continue to wiretap electronically scrambled messages and conversations. (Markoff, 1996)

As of March 1997, the Clipper Chip has yet to be implemented because of widespread protests from Internet users.

Moreover, creating policies for a new technology is difficult. For example, the University of Colorado has a standard policy on e-mail and its use for its four campuses; and yet, the individual campuses can create their own policies that best meets their needs. This is difficult because policy makers do not want to be too intrusive, but do want to protect students and the university.

Preserving privacy continues to concern Americans as more powerful technologies overcome the historic boundaries which maintained it: space and time.

(Katz and Tassone, 1990) Databases that store personal information allow people to rummage through a person's past and present for addresses, phone numbers, employment, education, and any other types of information that may benefit individuals, organizations, or companies. For example, health care practitioners are beginning to put medical information about patients on the Internet so other health care providers can access this information to provide better service to the patient. (*National Research Council, 1997*) The National Research Council also reports that this information is not as secure as one might hope and people's past, present, and possibly future can be interpreted with their medical records.

Americans may also be increasingly concerned because of the "new surveillance" technologies. These technologies are able to transcend "barriers and boundaries—be they distance, darkness, time, walls, windows, or even skin---that have been fundamental to our conceptions of privacy, liberty, and individuality." (Marx, 1990) This also holds true for Internet communications. E-mail messages can be intercepted by a system administrator or hacker while it sits on a computer. The Federal Trade Commission reports that 82% of Americans are worried "about personal privacy" on the Internet. (Fitch, 1997)

If privacy is a concern of Americans, then what protects privacy on the Internet? Are there laws and policies that offer some form of protection? Has behavior changed because of the new technology? Do pre-existing norms offer guidelines? These are the questions that I will address in the chapter, Constructing Privacy. But, I will first examine the literature about privacy, technology, and the Internet in the chapter, Privacy and Internet Communication.

2. PRIVACY AND INTERNET COMMUNICATION

There have not been many articles written on privacy and the Internet because the Internet is relatively new. But others have written on broader topics like privacy and technology. Even broader, are the theoretical models that I will use to explain behavior.

2.1. Theoretical Models

Ogburn (1966) theorizes that technology often develops faster than the policies that are supposed to regulate it, thus producing "culture lag." Cultural lag can be defined as "the gap between the technical development of a society and its moral and legal institutions." When a new technology generates popular use it takes some time for norms and values to develop (as well as laws and policies). For example, forwarding an e-mail to a third party may not be appropriate; especially, if the e-mail contains personal or sensitive information about the author of the original message. This is commonly referred to as "netiquette:" the *mores and norms* that regulate considerate and appropriate behavior on the Internet. (Wong, 1996) These take time to develop.

Another problem that the Internet creates for policy and lawmakers is geography.

> It (the Internet) poses cultural problems as information is made available regardless of social and cultural boundaries and the policies of nation-states. (Shields, 1995)

The United States and China may have conflicting laws about free speech on the Internet. Likewise, North Carolina and California may have conflicting views about the definition of Internet crime. Consequently, if a person violates a law in North Carolina, but is in California, can that person then be tried by the North Carolina law? As of March 1997, the Supreme Court will be deciding a similar case with the two states regarding pornography. (Interview) The Internet creates problems because a person with the

right equipment and software can access a lot of information from anywhere in the world. Ogburn would argue that privacy and privacy related issues are lagging because culture does not know how to deal with it.

On the other hand, Ervin Goffman would argue that time is not a major factor in determining actions on the Internet and theorizes that people are constantly trying to "present themselves to others in ways that are most favorable to their own interests or image." (Goffman, 1959) Two common terms associated with this theory is "front stage," and "back stage." Front stage "is the area where a player performs a specific role before an audience." And back stage "is the area where a player is not required to perform a specific role because it is out of view of a given audience." For example, a system administrator's front stage role is to obey the company's policies about not reading another user's e-mail message; whereas, the back stage role would be to read that user's e-mail message. Another example would be a hacker's front stage role of breaking into computer systems to prove his computer skills to his peers. While, his back stage role may actually be his quest for knowledge.

2.2. Privacy and Technology

Another related article is *Privacy and Technology* by Gary Marx. He provides ten reasons why privacy and anonymity are important. The following two reasons are most related to this work:

1. The ability to control information about the self is linked to individual dignity, self-respect, and the sense of personhood.
2. Anonymity can be socially useful in encouraging honesty, risk-taking, experimentation, and creativity.

Marx also offers suggestions on how to protect privacy. This includes the discussion of,

"public awareness," "Gross National Privacy Invasion," "code of ethics for professionals and service providers," "technologies," and "legislation." All of these are similar to the ones I will propose in the chapter titled Protecting Privacy.

In his book, Undercover, (Marx, 1988) defines the "new surveillance" as "powerful new information-gathering technologies…extending ever deeper into the social fabric and to more features of the environment." Moreover, Marx explains, "the new surveillance is relatively one-sided: it is likely to increase the power of large organizations, but not that of small ones or individuals." Corporations are generally the ones with the resources to gather information about Internet users.

In his book *Panopticon; or, the Inspection House*, Bentham describes the "perfect prison" where everybody would be under constant surveillance.

> Recent developments in telecommunications, along with other new means of collecting personal information, give Bentham's image of the panopticon great contemporary significance. (Marx, 1990)

The Internet has the potential to have everybody under "continuous surveillance." The technology exists for this to happen. But many would agree, however, that we are not at that stage of continuous surveillance (Lyon, 1993).

2.3. Internet Privacy

Much of the literature on Internet privacy addresses the need for anonymous communication in cyberspace. Barnes (1994) argued that free speech, the speed in which documents can be put on-line, and the "optimization of the users privacy" would ensure anonymity. Others have argued for increased awareness of users (Marx, 1994; Spetalnick, 1993; Borella, 1991; and Kapor, 1991). Spetalnick (1993) suggested that "the best hope seems be…to encourage members of the electronic community to define

and adopt for themselves standards of behavior that acknowledge individual and institutional responsibilities as well as rights."

Johnson (1994) argued that in order to achieve "civility in cyberspace" then anonymity must be abolished. The author argues that anonymity may lead to the escalation of illegal and harassing activity because the "ability to act anonymously, sporadically, in large groups brings out the worst in human character." (Johnson, D. 1994) The government would like to have access to e-mail because of the fear that anonymous e-mail will weaken national security.

On the other hand, Marx argued that "anonymity, involving the right to be left alone and unnoticed, has also diminished," with the new technologies. In turn, this will lead to decreased honest communication.

Moreover, the Electronic Frontier Foundation (EFF) is a civil libertarian web site that is oriented toward attaining the broadest Internet rights without intrusion from the government and third parties. The majority of articles argued that the Internet should be unregulated. (Johnson, 1994; Borella, 1991; and Morley, 1993)

2.4. Electronic Mail Surveillance

The Office of Technology Assessment (OTA) wrote an article titled *E-Mail Surveillance* that proposes a model for understanding how e-mail privacy can be broken. There are five ways in which e-mail can be read by a third party and these will be more closely examined when I propose my own model for e-mail interception in section 5.1. Electronic Mail.

3. METHODS

In the beginning of this research project, I wanted to examine the prevalence with which system administrators (SAs) read staff, faculty, and student e-mail. This was interesting to me because, as a student, I wanted to protect and learn more about student rights. But, I also wanted to understand the administration's perspective. Because there were so few SAs on campus that deal with e-mail, I broadened the scope of my research to beyond just SAs to include students and staff. Between September 1996 to March 1997, I collected data related to the Internet and privacy from students and staff at the University of Colorado. I used interviews and surveys to help me focus my research topic to privacy and the Internet.

3.1. Interviews

I used semi-structured interviews to gather data from managers of SAs, SAs, and police officers covering four different university departments. My initial questions included: Do SAs read other people's messages for fun? And if they do, why? Is it because they are bored? Or do they *not* read other people's E-mail because it is boring? Is there some monetary gain involved? Moreover, if they do read personal e-mail, what do they read? There are programs that can search for key words; do they use these programs to search for information they are interested?

Initially, I sent an e-mail to the director of the main computing center requesting to interview him. Because of his lack of time, he declined to be interviewed, but referred me to other people that could help me. These were people who had the greatest access to the e-mail machines on campus. Thus, I sent an e-mail to those SAs and managers and asked them if they had the time to be interviewed for my honor's thesis

(see Appendix 1 for content of e-mail). Most of the people I mailed were quite receptive and agreed to be interviewed. The people who declined to be interviewed felt that they did not have the time, nor the expertise, to answer my questions. Often, they would refer me to people they thought were better contacts and therefore my interviews snowballed.

Originally, I thought that there were more than ten SAs who worked at the main computer center; but, there were only four. Consequently, I expanded my research to encompass the whole institution; including, individual departments.

I interviewed twelve people. To ensure confidentiality, I told them that everything they said would be anonymous, meaning that I might quote them, but would not mention their names. The early interviews were more structured because I had set questions (see Appendix 2). But, I went away from this and tried to make it more like a "conversation." I would explain certain scenarios (e.g. if you saw in the message header, "I'm going to kill you," what would you do?) or mention key issues with the Internet, like privacy, free speech, and intellectual property and asked them to expand on these issues.

I also used the interviews to gather empirical data on the ways in which Internet technology itself protects or allows invasions of privacy. Although I learned some Internet technology through my work experiences, the interviews provided more information in which Internet technology could threaten privacy.

Lastly, the interviews provided information on the laws and policies that I analyze. The interview participants referred me to certain laws (e.g. Buckley Amendment) and policies (CU's "E-mail" policy) that might be beneficial to my research.

3.2. Surveys

I surveyed 184 students in a convenience sample of five Business and three Arts and Science courses. Females composed slightly more than half of my sample and more than half were between the ages of nineteen and twenty-one. I received the professors approval for administering the surveys by submitting a sample survey and explaining that the survey should not take more than ten minutes. I also explained to the participants that the survey was for my research and that participating was voluntary.

I selected the above classes because of easy access. Most of the classes that I chose to survey were ones in which I am a student or teacher's assistant. I waited a few weeks into the semester before approaching the professors of the class about administering the survey in their class.

Being a teacher's assistant also helped in administering the survey. First, I asked the professor if I could administer the survey and then asked my class if it was okay with them. I did not want to bias the information gathered in the survey, therefore, I left the room and had a student administer the survey. Also, being a TA gave me the chance to ask a second TA to administer the survey in his three classes.

The surveys addressed student expectations with regard to Internet rights (see Appendix 3 for content of the survey). The survey data helped me narrow my research topic from cyber-rights in general (free speech, privacy, and intellectual property) to Internet privacy. In addition, the survey data allowed for some means of comparing behavior between administration and student views on Internet privacy.

3.3. Data Analysis

I analyzed my survey data by first tabulating it by hand and then entering it into a statistical software program. This gave me simple percentages and allowed me to make graphs of my data. For my interviews, I would transcribe them using a word processing program and then I would organize the data into categories; for example, “privacy.”

3.4. Limitations

Self-reported data is one of the potential problems of my research. How can you trust self-reported data; especially, when people have things to hide? Why should anyone tell me the truth? In the beginning of my interviews, it seemed that participants were hesitant to answer my questions; but, I addressed this problem by assuring anonymity to the participants. And for the latter interviews, I told my participants that I was going to destroy the contents of the tape that I used to record our conversations. This seemed to ease the anxiety of the participants.

4. CONSTRUCTING PRIVACY

Privacy is a concern of people who use the Internet. According to a survey I distributed, 61% (n = 114) of the respondents were at least "slightly worried" about a "third party reading their e-mail." And the Federal Trade Commission reports that this percentage is as high as 82%. Thus what is privacy?

There have been many debates about the actual definition of privacy. According to Justice Brandeis, privacy is simply the "right to be left alone." Using this definition, unwanted e-mail advertisements could be a violation of privacy. The Cyberspace Law Institute and Counsel Connect define it as "the power to control what other people know about you." Herein lies a problem with privacy debates, there is no one definition. Nevertheless, I will use the above two definitions.

Privacy is protected on the Internet in many ways. Most existing policies and laws are meant to protect the user from unwanted intrusions. This includes federal and state laws. These laws deal generally with computer crime, but, some of them can be translated to the specifics of the Internet.

At a more local level, organizations have their own policies related to the Internet. CU has two policies to ensure appropriate use of campus computer resources: "E-mail" and "Responsibility of Users." Another way in which privacy is protected is normatively or users learn new manners. Users also normalize or accept the threat of privacy for a variety of reasons. The following addresses, in greater detail, how laws, policies, and norms establish and protect Internet privacy.

4.1. Laws

Implementing existing policies of older technologies with current technologies can

be problematic. For example, Johnson (1990) compares the Internet to the telephone and postal mail. The Internet is similar to the telephone in that it uses telephone lines. According to Johnson e-mail messages are like voice mail messages. System administrators can act like telephone operators and laws should treat it that way.

On the other hand, the Internet is similar to postal mail in that the messages are in text format. In this sense, SAs are like postal inspectors, and a common argument is that e-mail should be regarded as First Class mail. But the most obvious difference (other than that e-mail is in electronic form) is that when postal mail is sent to the wrong person, most people would return it without opening the letter. With e-mail, however, the letter must be opened in order to determine that it was sent to the wrong person. This is part of the reason why e-mail is considered like a "post-card."

As a result, people are trying to use old solutions to solve new problems.

> Since electronic communication can be seen to have the properties of private conversations, street speech, postal mail, printing, broadcasting, and common carrier telephony, each with a different legal position with regard to communication rights and First Amendment freedoms, the appropriate choice of metaphor is of real consequence. (Smith, 1996)

Unfortunately, the Internet is more complicated than the above examples and thus policy and law makers are having a difficult time creating rules and regulations for the Internet. Below is a small, but important, sample of existing policies that deal with the Internet.

4.1.1. Family Educational Rights and Privacy Act of 1974 (Buckley Amendment)

One administrator informed me that "the Buckley Amendment is what makes reading student e-mail illegal." (Interview) The Buckley amendment simply states that students have the right to protect academic and other information from third parties

(including parents). Unless there is a strong administrative reason to view a student's grades, most people do not have a right to see them.

This law has been extended to cover student e-mail. According to my survey, more than half of the respondents believed that parents should not have the right to view student e-mail messages if that student passes away. System administrator's can view messages if there is an administrative concern, but are legally prohibited from disclosing the information to a third party.

4.1.2. Electronic Communications Privacy Act of 1986 (ECPA)

Technology is constantly outpacing laws and therefore Congress wanted to create a law that would "safeguard the right to individual privacy from erosion due to technological advancement." Moreover, the law "extended Fourth Amendment protection to new communication technologies such as cellular telephones, data transmissions, and electronic mail" (Moreley, 1993; Beeson, 1996). This law regulates SAs. For example, the ECPA forbids the "unauthorized disclosure of the content of communication" by the SA. (Johnson, 1990; Beeson, 1996)

4.1.3. Colorado Computer Crime Statute

Colorado has its own computer crime law that could protect people from abuses on the Internet. For example, "using the property or services of another without authorization" could be interpreted as using another person's e-mail account without his permission. (see Appendix 4 for content of Computer Crime Statute) But as one police officer told me

> There is a statue about computer crime in Colorado that lumps a lot of things together, but a lot of times the specifics aren't there.

The same police officer said that if a crime is believed to be committed on the Internet,

the easiest thing to do is to use an existing law to arrest the person. For example, if a person is trying to commit credit card fraud over the Internet, the police will generally ignore the communication's medium, but will arrest the person based on existing laws on fraud.

4.2. Institutional Policies

The policies I examine are CU's E-Mail and Responsibility of Users policies. Both of these policies were an attempt to "keep up" with the times.

4.2.1. CU's E-Mail Policy

Staff and faculty are considered employees of the institution, whereas students are considered clients of the institution and are protected by the Buckley amendment. The creators of CU's E-mail policy understood that the Buckley amendment applied to student e-mail, and thus made certain that the policy did not violate the law.

Staff and faculty, by policy, should only use CU's equipment for the institution's affairs; otherwise it can be deemed a violation of policy. But the institution decided that this was impossible to detect and punish because of the magnitude in which the institution's equipment is used for personal reasons. For example, "staff and faculty are allowed to use the phone in their office to make an appointment with their doctor, as long as it is a local call, but are not allowed to bill the university if the phone call is long distance." (Interview)

CU could easily deploy a policy that states that e-mail is not to be used for personal reasons; but decided that it would be too difficult to implement. On the other hand, many companies have a strict e-mail policy stating that e-mail should only be used for business purposes. Students do have the right to use e-mail for personal

reasons, without fear of any consequences. As long as they do not break the law, or "make the institution look bad" then they can use e-mail as they so choose. Again, this is partly because of the Buckley amendment which is a federal law protecting sensitive information of students. If SAs are paid to look for certain things in people's e-mail then they would be considered an Internet service provider. Consequently, the workload and resources of this institution would also increase.

For example, a person who received a threatening message forwarded a message to a SA. As of March 1997, this is still under investigation. The police officer on the case filed for a search warrant to view an Internet service provider's e-mail logs. But, by policy, this message would never have been noticed by any SA because, in theory, they are not allowed to search for specific content of an e-mail message. According to my survey, over 60% (n = 112) of the respondents agreed with this policy by stating that if a SA, by accident, saw a message header of "I'm going to kill you" he should *not* report this to his superiors or to the police. But, because the message had been brought to the attention of the SAs and the police, they began investigating the incident. Moreover if a private citizen reports an illegal activity to the police then the police can investigate.

CU's E-mail policy was made to be broad. (Interview) The original developers of the policy wanted to protect students and inform them of the security problem with e-mail. One of the first things SA's told me in the interviews was that e-mail is not a secure document and it resembles a "post-card." Even if every SA at CU chooses not to read people's e-mail, the message can be read by different SAs at other institutions. This is because the Internet is a network of computers and if one network goes down,

then the e-mail messages are typically re-routed to its destination.

4.2.2. CU's Responsibility of Users Policy

This policy states that people using "computing and networking resources at the University of Colorado at Boulder" should realize that this is a privilege and it should be used in an "efficient, ethical, and legal manner." In terms of privacy, the policy states that "users shall not intentionally seek information on, obtain copies of, or modify files, tapes, passwords or any type of data belonging to other users unless specifically authorized to do so." If these rules are broken, it "may result in the suspension of computing privileges; disciplinary review, which may include the suspension or expulsion from the university; termination of employment; or legal action." A police officer told me that,

> The university has a little more leeway in disciplining people because…if somebody uses e-mail and violates one of those rules, even if they don't break any laws, the university can bring sanctions against the student.

Being responsible about using computer resources on campus is not the only way of protecting privacy. Users learn new manners with the new technology.

4.3. Normative Behavior

According to my survey, there is a normative understanding not to violate a person's privacy. For example, 62% (n = 115) of my sample answered they would "log the person out" if that person was still logged in, while, 26% said they would do nothing, and less than 10% said they would "look through their files" or "play a joke." A person is "still logged in" if he leaves his e-mail account open which can be used by anyone who walks by the terminal. Moreover, the e-mail account is vulnerable because passwords can be changed, e-mail messages can be read, and files can be deleted. To "log a

person out" would probably benefit the individual who unwittingly or accidentally left his e-mail account vulnerable. The majority of the survey respondents have either learned new manners regarding the Internet or are uncomfortable in violating another person's privacy because of their beliefs and values.

4.4. "Anonymity is part of the Magic" (Myers)

Marx (1988) argued that anonymity is important in protecting an individual's identity. This is shown with the Internet because information about a user can be gathered without his consent and thus he cannot protect information about him. One way of doing this is using Netscape. By entering a return e-mail address, Netscape allows a user to send e-mail to other people. The program, however, does not verify the e-mail address. In other words, the person can easily use a false name and address -- also known as "piggy backing." (Parker, 1976)

Of course total anonymity may lead to irresponsible behavior; such as, sending threats over e-mail. But, anonymity is beneficial in terms of letting users freely use the Internet without fear of someone watching them, or entering data that can identify them. There are two forms of anonymity: institutional and technological.

4.4.1. Institutional Anonymity

Being associated with the University of Colorado can create an "invisible" surfer on the web. For example, a web site may interpret that I am "associated with the University of Colorado" and that I am "coming from tele-anx0117.colorado.edu." But, this could be hundreds of people. This information does not expose who I am and where exactly I am coming from. (Please see section 5.2. World Wide Web for more information)

Another source of anonymity that the University of Colorado provides is the use of the labs available on campus. It is impossible for a company to identify the user if the information gathered states that the person is using machine #40 in the Engineering lab. The company could speculate that the user is a college student, but there are no specific details given about the user.

4.4.2. Technological Anonymity

There are other means of ensuring anonymity, such as anonymous e-mailers and re-mailers and anonymous URL sites. Anonymous e-mailers are e-mail servers that allow people to send messages using fake or unidentifiable e-mail addresses. Anonymity can be important in allowing for honest communication. A police officer told me that there have been some professors who complained to the police because they received an anonymous e-mail. The police looked through the content of the messages and found that the messages were not threatening, but, were critiques of the professors and their teaching style. Anonymous e-mail allowed students to voice their opinions about their professors without fear of being punished.

On the other hand, an example of where anonymity can be harmful is the case where a student sent an anonymous e-mail to a class e-mail list telling the students that everyone has received A's and to not come to class anymore. A SA was able to track the student down because he dialed into CU's network from home. Consequently, he was expelled from CU.

Finally, there are web sites that allow users to shield their identity when they visit a web site. The "Anonymizer" web site allows a user to do this. (www.anonymizer.com)

> If you begin each trek on the Web by signing up at The Anonymizer site, its address is the only one that will show up in the server logs no matter

where you go. (Fitch, 1997)

For more detail on how visiting a web site may identify a person, please visit the section 5.2. titled World Wide Web. Although most of these sites do work, their effectiveness is unclear.

4.4. Awareness of Privacy

Normalization is the time needed for people to cope with change; especially with technology. Marien (1997) argued that "privacy is a cultural construct, and maybe we'll learn to live with this new invasion, even with cameras on every lamppost." He was primarily speaking about the Information Age, but, could have easily have been translated into Internet terms. Obviously, the Internet is no different and according to my survey, users fall into three groups about their perceived threat to privacy:

1.) People who believed that their e-mail was likely read by a third party
2.) People who believed that their e-mail was not likely read by a third party
3.) People who believed that their e-mail being read by a third party was impossible

4.3.1. People who believed that their e-mail was likely read by a third party

This group comprised 47.8% of my sample (n = 88) and can be divided into two more groups: people who are concerned with their e-mail privacy and people who normalize the privacy invasion. Fifty-five people were concerned about their e-mail privacy being invaded and were worried that their e-mail was read by a third party.

The second group (n = 33) normalize the privacy threat because they realize that the Internet is a communications medium that is vulnerable. These are the users who value what the Internet brings and do not feel that their privacy is being invaded or do not care. These people thought their e-mail was likely read by a third party, but, were not concerned.

4.3.2. People who believed that their e-mail was not likely read

This group also equaled 47.8% of my sample (n = 88) and again can be divided into two more groups. Forty-nine people believed that their e-mail was not read by a third party and were not worried. This could be interpreted in many ways. First, they could believe that their e-mail is a secure document and cannot be read by a third party. Second, they may not know the ease in which e-mail can be intercepted. Third, they do not care whether a third party reads their e-mail.

The second group (n = 39) felt their e-mail was not likely read, but, were slightly worried about this. This could be because the respondents felt that the majority of their messages were not read by a third party; but, believed that there was still a small chance that it could be. A student wrote to the side of this question, “At least not at this time. My mail is not that confidential, but may be in the future.” In this case, the student felt that her messages were not read because the content of her messages were not important. This student and could be an explanation of other students in this group, equated violations of privacy to importance of her status or her messages. Thus privacy is not the "right to be left alone," or "controlling information gathered about oneself;" but, the importance of the e-mail message.

4.3.3. People who believed that their e-mail being read by a third party was impossible

This was the smallest group in my sample where 1.6% (n = 3) felt that a third party reading their e-mail was “impossible” and were “not at all” worried. These three people used e-mail, “occasionally” which could explain why they were not worried about having their e-mail read by others. Another explanation is that they did not feel that

their e-mail was important enough to be read by someone else.

Thus what kind of breaches of privacy occur on the Internet? How intrusive are they? How prevalent? Do the above protections work? The chapter, Technological Breaches of Privacy, will address these questions.

5. TECHNOLOGICAL BREACHES OF PRIVACY

There are many forms of privacy breaches on the Internet. E-mail can be intercepted by third parties for a variety of reasons. The World Wide Web and Unix commands can be potentially intrusive. For example, the address, phone number, and e-mail address of a person associated with the university can be gathered using the 411 command. The following is an examination of how privacy can be breached on the Internet.

5.1. Electronic Mail

The Office of Technology Assessment argued that there were five ways in which e-mail can be read by a third party:

1.) At the terminal or in the electronic files of the sender.
2.) While being communicated.
3.) In the electronic mailbox of the receiver.
4.) When printed into hard copy before mailing.
5.) When retained in the files of the E-mail company for administrative purposes.

Although this model brings up good points, below is an alternative model that I will propose.

1.) In the server or machine where the e-mail sits
2.) While the e-mail is in transmission
3.) Error in transmission
4.) E-mail commands
5.) E-mail message is printed out

5.1.1. In the Server or machine where the e-mail sits

OTA argued that e-mail can be intercepted “at the terminal or in the electronic files of the sender.” But e-mail can be intercepted on the server or machine where the mail is stored. This includes OTA's first, third, and fifth points: an e-mail being read “at the terminal or in the electronic files of the sender”, “in the electronic mailbox of the

receiver", and "when retained in the files of the e-mail company for administrative purposed." Thus an e-mail that sits on a server or machine can be accessed by SAs and hackers.

Most e-mail programs allow users to save messages. The saved messages sit until the owner of the e-mail account deletes them and until then are susceptible to interception. Both hackers (potentially) and SAs have access to these messages. Hackers have access because of illegitimate means, and most of the time, SAs have access because of legitimate means.

Furthermore, during the time a person types a message, a curious person could read the message over the shoulder of the sender. This is more prevalent in computer labs then at a work place because of the proximity of the computers. For example, most computers in the computer labs on campus are in rows of four to five. Generally there is not much space between the computers; nor, is there a divider that blocks people's view.

5.1.2. E-Mail can be intercepted during Transmission

OTA argued that e-mail can be intercepted during transmission. E-mail is sent through telephone lines and thus could be intercepted. Most messages, if sent to another school, must go through many "gateways" or places where a machine sits and directs the message to the right address. E-mail is sent via "packets" and could be intercepted by hackers. But, one hacker told me, "this is extremely difficult to do, unless you had the right equipment." (Interview) Packets are difficult to intercept because they are like a puzzle. An e-mail message may be separated x number of packets (x depending upon the size of the message). Therefore, ten packets could be one e-mail

message. Thus, a person could intercept one or two packets, and still would not understand the entire e-mail message.

5.1.3. E-Mail can be intercepted when printed into hardcopy

Another point OTA argued was that e-mail can be intercepted "when printed into hard copy before mailing." Potentially, a person could receive an e-mail then send it out via postal mail. People do print e-mail messages for a variety of reasons and the printout could be intercepted quite easily. Most SAs agreed that this is probably the easiest form of reading another person's e-mail. This is because when an e-mail is printed, it sits in the print queue, then when it is printed sits in the printer, and finally it could sit on a person's desk. A person who is knowledgeable about networks could view the message from the queue. Moreover, when the message is finished printing, it could be picked up by a third party because the person forgot that he printed his message. Finally, someone could read the message while the printout sits on a person's desk or dig it out of the trash or recycling bin. Of course a printed e-mail message could be shredded, but printing is still the easiest form of interception by a third party because it does not require a lot of technical knowledge.

People could also accidentally print to the wrong printer. For example, if a user does not set his print settings correctly, his message could be printed to a different building that is across campus. Obviously, someone at that building could pick up the print out and read it.

5.1.4. E-Mail Commands

Forwarding a message is another way in which e-mail may be read by a person for whom the message was not intended. There are some messages that people do not

want others to read. People can forward a message accidentally or without consideration for the privacy of the original author of the message. For example, students in my recitation send me e-mail messages about concerns they have with the recitation. I would violate their privacy if I were to forward their message to the whole class list (over four hundred students). The ease of forwarding a message allows for e-mail to be read by a third party.

Another way is the Blind Carbon Copy (BCC) command. Most e-mail applications allow people to send carbon copies of a message to another person. This is a useful command because it saves a person typing a message over and over. The BCC command allows a person to send a carbon copy of a message without the knowledge of the original intended recipient.

> If, I did a CC (Carbon Copy), you would have seen it, a third party was getting a copy of the message. But, with a BCC you would have never known that, and I have to admit there have been quite a few occasions where I have used the BCC feature to keep a third party informed without letting the original person I am e-mailing know. I basically kept that information away from them and thereby possibly misleading them into thinking they were having a privileged conversation with me, but in actuality that wasn't happening at all. (Interview)

As the person I interviewed said, "it's basically like eavesdropping in a sense…it would be like me calling you on the phone and having somebody pick up on the extension." Similar to forwarding a message, there is not a way of finding out if a message has been sent in BCC mode.

Hiding who you send messages to is another possibility of BCC. This is done by putting all of the e-mail addresses in the BCC area and the message will be sent with an "undisclosed recipients" header. Thus a user could protect the recipients' identity.

5.1.5. Error in Transmission

Finally, a message may be sent to the wrong address or there was an error in transmission. This could be on the users end who accidentally types in the wrong address or accidentally sends a message to the entire e-mail list; instead of to just one person. The system could also deliver the message to the wrong person. Either way the message is being read by a person for whom the message was unintended. E-Mail is not the only means in which information about the user can be gathered. The World Wide Web is another Internet medium where users are not anonymous.

5.2. World Wide Web

The Internet is a communication's medium where information is readily available. This also includes information on the users who browse World Wide Web sites. According to the Center for Democracy and Technology (CDT) not many people are aware that information is gathered about a user.

5.2.1. The Internet "Voyeur"

Many people believe that "surfing the Net" is private. This is because you cannot see the third party intercepting the data from you. People do not realize that there are web sites (Magellan) that will randomly select what users have searched for; allowing people to trace the steps of a previous user.

> Every 20 seconds, the Magellan Voyeur page gives a random sampling of keywords that other visitors to the site are requesting from the Magellan search engine. Click on these links and you can see the results of someone else's searches. (Hawn, 1997)

Privacy concerns are evident since many people do not believe that their inquiries about certain topics would be made public. Although not every search engine does this, it is common that companies keep a record of people's Internet use. "Although it may not seem like it, someone is following you through cyberspace. Every time you retrieve a

file, view an image, send an e-mail message or jump to a new web site, a record is created somewhere on the Net." (CDT).

Many people believe these voyeuristic tendencies are perfectly acceptable because they believe that the Internet is a "public forum." Thus, people who use the Magellan search engine should realize that their searches are not private.

On the other hand, privacy is a value that everyone should adhere to because without privacy, "people are in a sense turned inside out." (Marx, 1990) Moreover, Internet security seems lax at times because there are users who are knowledgeable enough to manipulate their identity. Therefore an e-mail message with my address on it may actually be someone else disguising himself as me or someone who is using my e-mail account. Thus, information gathered about me may be incorrect.

Of course having too much privacy can lead to consequences. Complete anonymity can shield irresponsible and inappropriate behavior.

> New opportunities and temptations for deception and rudeness are provided by technologies that offer remote access and anonymity. The absence of visual or auditory cues makes it easier to conceal, deceive, and manipulate. The isolated individual sending messages at a computer terminal or responding to the requests of an electronic voice may make it hard to remember that there is (or will eventually be) a human being at the other end. The emotionless quality of the medium, the invisibility of the other, and the anonymity of the sender are not inherently conducive to civility. (Marx, 1994)

Hackers already have a lot of power in terms of being able to manipulate computer systems to their benefit. Having complete anonymity may lead to more harm done to computer systems and in turn people's privacy may be violated.

E-mail messages would be harder to trace. Breaking laws would be easier if there was complete anonymity. For example, a user could send an e-mail

advertisement about child pornography and would not worry about getting caught. Sending threatening letters would also be easier. A death threat to the president would be untraceable. "Flaming" or verbally abusing someone over e-mail may increase. Thus, laws and policies would be harder to enforce if a person could shield his identity.

But, protecting privacy is important on the Internet. "The abuse of privacy of individuals comes about from unrestricted collection of data about people, from storing inaccurate or incomplete data, from its unauthorized disclosure, and from incorrect or otherwise harmful conclusions drawn from it." (Parker, 1976 - p. 239) Privacy and anonymity help individuals protect their identity, who they are, and what information is gathered by others.

5.2.2. A Sticky Web

Another privacy concern is that some companies gather information from people who visit their website. For example, certain websites are able to locate where a person is coming from and what programs a person is using. This is shown when I visited the CDT's homepage:

> You are affiliated with University of Colorado.
> Your computer is a PC running Windows 95.
> Your Internet browser is Netscape.
> You are coming from tele-anx0117.colorado.edu.

I did not provide this information voluntarily, but, the computer on the other end interpreted this information. As CDT points out, this is just a small piece of information that they provided to enlighten visitors of their website.

> As a small non-profit public interest organization, CDT's web pages reside on a server run by our Internet service provider, and as a result, our ability to collect even more revealing personal information than what is displayed above is limited. However, a web site operator with the right equipment and the desire to do so can easily obtain your e-mail address, the exact

> files you viewed, and other detailed information without your knowledge. And you reveal information to web site operators both directly and indirectly.

The ease with which data is collected about users of the Internet is a tribute to the age of information gathering, where trivial and unimportant data can become important to certain types of groups or people. (Marx, 1988) The information gathered can easily be sold to marketing companies, can be used to show what programs people use, and the location of a person.

Another example is the creation of a File Transfer Protocol (FTP) log. Simply put, FTP logs label what files users download or upload and where the files are put. Below is a sample of an FTP log:

> 97.02.09 21:07 B C:\John\CLASSES\Honors\Outline of Privacy.doc --> eddie.colorado.edu /home1/jwong/Honors Outline of Privacy.doc
> 97.02.09 23:18 B C:\John\CLASSES\Honors\Methodology.doc --> eddie.colorado.edu /home1/jwong Methodology.doc

The date, time, where a user puts the file, and where a user got the file is provided in these logs. Every single time a user downloads a file, it is added to a FTP log. This log is created on the person's computer and also on the corresponding computer.

5.2.3. Cookies

Cookies are programs that are embedded in a user's web browser that allow SAs and/or web masters to view certain types of information. The most common forms of information gathered are the number of times a person visits a company's website. Thus a "Cookie" acts like a counter.

Marx (1988) argued that the "new surveillance…is likely to increase the power of large organizations." That is, companies with the resources and knowledge are able to monitor the number of times a person visits their website and thus could sell this

information to marketers along with other personal information. Companies are unable to obtain more personal information, like your name and phone number. (Caruso, 1996) This is not to say that the technology is not moving toward that direction.

Cookies are frequently used by companies to gather information for their advertisements:

> When a user visits AltaVista…a cookie is stealthily sent along with that site's images, and the information is stored in a database on a remote server at DoubleClick. This worries some users, who feel like they are being watched, and fear that anonymous database entry will be used to build a profile of their likes and dislikes. (Glave, 1997)

Cookies are yet another way in which a user's privacy can be violated and used for the benefit of companies.

Web monitoring tools are not the only way in which privacy can be violated. Unix commands also give a lot of information about people and are available to everybody using an e-mail account at CU.

5.3. Unix Commands

Technological invasions of privacy are available to everyone who uses a Unix based e-mail account and generally are easy to learn. Unix commands are like the caller ID service that telephone companies provide: they can provide the name, date, time, and the location from which the user is operating. And like the caller ID service, most people are unaware that they have left any information by contacting someone.

The most popular e-mail machines that faculty, staff, and students use are run off of a Unix server (e.g. spot, ucsu, ucsub, and rintintin). And, there are some Unix commands that allow people to query or "finger" another person for general information or find when they last logged in and for how long using the "last" command. Here is an

abridged list and description of commands that people can use as “surveillance” or caller ID tools in Unix:

5.3.1. Finger

To use this command a person would type “finger somebody@somewhere” and generally information will be returned. At CU, this information includes name (you can create a psuedo name), phone number(s), plan, login name, and the time I have been logged in. All of this information is displayed if the person who is “fingering” is on the same machine as the person who is being “fingered.” On the other hand, if the two people are on different Unix machines then only some information is given (e.g. login name, name, when and where the person logged in). There are harmless information displayed because people voluntarily type in information they want displayed. For example, I put in a phone number that I can be reached at; otherwise, no information would be present.

5.3.2. Last

The last command allows people to investigate the x number of times people have logged into their e-mail account, when, and where. This command only works if the two people are using the same Unix machine. For example, if I am on a ucsu account, then I can only use the last command for another person who is on ucsu.

The last command can almost be used as a tracking device. The third column of information gives where the person logged in (e.g. from home, or any building on campus with the exact machine number), the date and time, and how long the person remained logged in. Obviously, a person trying to locate another person can use the last command to locate where the person is.

5.3.3. Grep

This command allows a person to research the last commands a person entered. This can also search out keywords like login names, words, and passwords. This is a popular command among hackers because they can search out loopholes in the system. As one hacker showed me, he found people's passwords to their accounts by using the grep command. (Wong, 1996)

5.3.4. 411

A 411 search at CU will reveal quite a bit of information. This reveals your name, e-mail address, address or campus address, phone number, department the student works at, the title, major and home page address. There is a way of changing any information in a person's 411 by calling the number in the disclaimer window. Interestingly enough, any marketer is privy to this information because CU is a public institution and must give this information to people or organizations. There is no cost for per student information, except, the labor to retrieve this information. (Interview) Lastly, this information is available to the information operators at CU (when you dial 492-1411).

Basic Unix commands allow normal users to trace and track people down. Moreover, personal information can easily be gathered and used by advertisers and organizations trying to sell products to people by sending e-mail advertisements or "junk e-mail." Obviously, personal information can be used correctly, but, also has the potential of harm.

If breaches of privacy do happen, what are the reasons for them? Is it because of boredom? Fun? Is it someone's job to read other people's E-Mail? Why do people

invade privacy? The chapter, Reasons and Justifications for the Breaches of Privacy will examine these questions.

6. REASONS AND JUSTIFICATIONS TO BREACH PRIVACY

Even though privacy is protected in certain ways, there are always chances to violate that privacy. Sometimes the violations are against policies and laws, while the majority of time, the invasion of privacy goes unnoticed. This is not to say that these invasions are ethical or should be ignored. For the most part, violations against policies and laws occur with hackers and SAs.

There are times when hackers break the law or an institution's policy when they violate a user's privacy. For example, altering or damaging files off a person's e-mail account is considered a crime in the state of Colorado. Hackers may violate CU's E-Mail policy when they read student e-mail messages.

Not only do users of e-mail have to contend with hackers who can break into a user's e-mail account; but, also with SAs who "have the keys to the kingdom." (Interview) System administrators have "superuser" access. Superusers can view and maneuver in and out of somebody's e-mail account with or without their consent.

At CU, most SAs follow the e-mail policy outlined by the main computing center which states that they should not read any e-mail without administrative reasons. Obviously, not every SA follows protocol. There are differences between what is policy and what actually occurs. Managers or supervisors want to believe that their SAs are doing the right thing; but, managers cannot keep track of every action of their SAs.

Most of the time, privacy invasions occur because they are legally allowed on the Internet. For example, e-mail logs are kept by certain companies and FTP logs tell what files were downloaded or uploaded by a person. For the most part, these logs help SA's in dealing with their machines, but, these logs also reveal a great deal of

information about a person. Moreover, common users can use certain Internet commands to search out people. As shown in the previous chapter, the invasions of privacy can occur frequently on the Internet. But, what are the reasons and justifications for the invasion of privacy?

6.1. Fun & Challenge

Typically, if people are afraid of their messages being read by a third party, more than likely, their fear points to hackers. Hackers are people who possess an incredible amount of knowledge about computers and the Internet. Many hackers search for security holes in computers and networks because they want to have fun and it is a challenge.

For example, a hacker can use the "grep" command to search for key words. One possible search is to look up "password" and hope that a person has unwittingly left their actual password in a file saved on their account. This way a hacker does not have to painstakingly find security holes in a system, but walks through the front door. (Interview)

Another example is a hacker "fingered" a user of another college and noticed that person had information about a favorite musical band in their finger information. The hacker was able to guess the password of that user based on that information. He then used the person's account to download pirated software. (Wong, 1996)

6.2. Boredom & Curiosity

Boredom is another possibility where a person can violate a user's privacy. Below is an excerpt of an interview with a SA.

> "Check this out," he replied. He then typed some Unix commands and the computer screen scrolled with e-mail messages. He told me that this was

> all of the e-mail messages of his department. I asked him why he was reading other people's mail and he told me that "I was bored one night, around 1:30 in the morning, and thought, why not?"

The SA was bored with work and wanted to read his co-worker's e-mail messages.

Although boredom itself can lead to a SA violating another person's privacy, boredom can lead to curiosity. The same SA was curious about what his boss wrote in his e-mail messages because his job performance evaluation was coming up. He did not find anything "interesting" with his boss's or co-worker's e-mail messages and thus only reads their messages "once or twice a month."

6.3. Duty & Responsibility

For the most part, SAs report only viewing user's e-mail for administrative reasons, for example, up keeping the e-mail server or by court order. If they view a message for a reason other than up keeping the e-mail server they must fill out a consent form from their manager (see Appendix 6 for concept and content of the consent form).

The most common administrative example is a SA who is the Post Master and has to redirect or figure out the intended recipient of an e-mail. According to one SA, he gets about a dozen to two dozen lost e-mail messages a day. A SA inspects the subject heading to decipher the identity of the intended recipient. There are times, however, when the SA must read the content of the message. Unfortunately, the content may contain sensitive information.

For example, one SA at another college received a message that could not be sent because the address was wrong. The SA tried to redirect the message, but failed because the subject heading did not contain sufficient information. Consequently, he

had to read the message. The message was about the sender hating her work and wanting to quit. The SA at the college did not want to forward the lost message to the company's SA because then the woman might get in trouble. Therefore, he contacted the woman and notified her of the lost e-mail. The woman was grateful that the SA did this because she was protected from a "possible awkward situation." (Interview)

Trust is placed upon SA's because they have complete access to the e-mail machines. In order to protect privacy of users, SA's not only need to follow policies, but, also respect the user's privacy. Most SA's want privacy for users because they do not want others reading their e-mail messages. (Interview)

6.4. Technological Superiority

There are some hackers and SAs who believe that most people do not "deserve" to use the Internet because of their "ignorance." (Interview with a hacker, 1996) The same hacker said, "if people are not bright enough to secure their e-mail account then why shouldn't I or another hacker take advantage of them." This hacker felt that he was justified to view other people's e-mail messages because he knew more than them. Similarly, the SA who read his boss's e-mail felt the same way:

> Aren't you scared that you're going to get caught?" I asked. "Not really. I am pretty much the only person who knows anything about Unix in my department and I can hide my tracks pretty well.

Technological superiority may lead someone to violate a user's privacy and may act as a protective barrier to being caught.

6.5. Accident

Another reason to violate a person's privacy is by accident. For example, a SA saw a message that entailed sex and started reading it. Before he knew it, he read the

whole message and “knew more about a person than he wished to.” Another SA said the message “was just there in front of me,” and “I couldn’t help it.” Even with current policies specifically stating that SA’s should not read other user’s e-mail messages, it occurs because SAs have easy access to other people’s e-mail.

6.6. Interpretations of Policies

CU’s policies were created to protect students and the university. But because these policies can be ambiguous, different interpretations may result. Consequently, privacy may be violated. Technology is definitely moving faster than the policies. Almost everyone I interviewed agreed that no one really knows the correct course of actions to take because people may interpret the current policies in different ways. “I may think this way, but, another person may think another.” (Interview)

6.7. Profit

Internet privacy can be violated because companies want information about Internet users. What files do people look at? What files do they download? When do they surf the Net? How many times do people visit web sites? All of these give an excellent description of users. Cookies provide information about users, which companies can in turn sell for a profit.

Sending mass e-mail advertisements (“spamming”) to people who frequently visit a company’s web site can be one way in which information can be sold. I received an e-mail that said:

> Privacy Alert: Did you know your Email address is publicly available?
>
> If you're aware of this fact, kindly disregard this message; otherwise, please note that it's been published on an unprotected, openly-linked web-page, that any person or program can access at:

http://rintintin.Colorado.EDU/~jwong/

A program goes through a web site searching for this information. Instead of being a "privacy alert" e-mail, this could have easily been an advertisement.

As shown, breaches of privacy occur. But, how can normal users protect themselves from having their privacy invaded? Are there technical fixes? Will technical fixes undermine the communication medium? Is the answer laws and policies? What can people do to understand the issue better? In the final chapter, I will recommend how to protect Internet privacy using Gary Marx's model of "privacy protection measures."

7. PROTECTING PRIVACY

The need to protect privacy is imperative in the Information Age as personal identity and information gathered about a person should be controlled by the user. The last sections of Gary Marx's article, *Privacy and Technology* provide these steps in protecting privacy: "public awareness," "Gross National Privacy Invasion," "codes of ethics for professionals and service providers," "technologies," and "legislation." These steps can be translated to protecting Internet privacy.

7.1. Public Awareness

A large percentage from my sample reported never reading CU's E-mail policy. Subtracting those who reported they have never used e-mail before, the percentage is 70 (n = 128). This could be because "it (e-mail policy) is not shown to people who acquire an e-mail account and thus people do not hear about it." (Interview) Reading this document may help students understand that e-mail is not a secure document because it can easily be read by others. Moreover, this document will also help students understand their rights as a student and the rights of the university. Further exploration may lead students to read the Buckley amendment, which protects not only their e-mail, but also their grades.

Finally, staff and faculty should be aware of what their rights are in terms of being state employees. Again, students, staff, and faculty have different rights because students are not state employees.

7.2. "Gross National Privacy Invasion"

This step is a measure of how frequent the invasion of privacy occurs. This could easily be translated into how often web sites keep track and gather information

about its visitors. As I mentioned before, there are Internet activists that are "rating" web sites on what information is gathered. Therefore, users may choose not to visit sites with "bad" ratings. Moreover, a common program that people use to browse web sites, Netscape, is changing how cookies are sent and distributed. In the future users would be able to control the information and distribution of cookies. Knowing the frequency in which privacy is invaded will allow people to understand how their privacy is threatened.

7.3. Code of Ethics

Almost all of the SAs agreed that their profession needed a code of ethics. Similar to other professions, a code of ethics would be guidelines that SAs follow in certain scenarios. Although codes of ethics in other professions are constantly broken, many felt that a code of ethics for SAs would help deter unnecessary stress regarding viewing other people's e-mail and minimize the occurrences of misinterpretations of policies. (Interview) A code of ethics then should encompass specific details of what is right and wrong.

7.4. Technologies

On a more technical level, there are encryption programs, such as Pretty Good Privacy (PGP), that enable a user to protect the content of their messages. This is because the sender of the message sends a "key" to the receiver, which allows the receiver to have the only access to that message. Unfortunately, PGP and other encryption programs are difficult to learn and thus not many people use them. Although a manager of SAs at CU told me that in the next two or three years, all e-mail messages will be automatically encrypted. The current problem is lack of resources.

There are technological means that may solve the awkwardness SA's must go through in order to redirect a message. One way is to completely automate the e-mail duties of SAs. If the program is not able to redirect the message then that message is deleted, saving SA's the trouble and moral dilemma of reading an e-mail not addressed to them. This already occurs in one department on campus. But, this solution contains flaws. The messages that are deleted will never get to their destination and thus the communication is lost.

Another way is to only show the header of an e-mail message. If the SA cannot figure out who the message belongs to by deciphering only the headfer, then he deletes the message. This can be possible by encrypting the message body, but, leaving the message header "public." For example, if a person sends a message with the header "Graduate Application Request," then the SA can safely assume that the message should be forwarded to the Graduate Admissions office; even though, the body of text is encrypted.

Increasing Internet security has always been a concern and can be done with the use of technology. Hackers and even intermediate Internet users are able to break into systems and cause havoc. In one case, a person not associated with the university was able to obtain the "superuser" password at CU. This means that the person had the equivalent power as a SA and was able to go through people's e-mail accounts without their knowledge. The obvious threat to privacy and security is evident in this case. Therefore, for protection, the superuser password is changed every semester at CU. (Interview)

But, e-mail is not the only security flaw that needs to be improved. Web

browsers, such as Netscape and Internet Explorer have been proven to have weaknesses. For example, a SA could use a loop hole in the Internet Explorer program and have remote access to the user's computer. (Klass, 1997) Another example is using a loop hole within Netscape, which allows a person to have access to e-mail sitting on a person's computer, even if the messages have been "deleted." (Stutz, 1997; and Wayner, 1997)

7.5. Legislation

New legislation is required for the Internet. Policies and laws can have a deterrent effect in stopping people from committing crime or breaking school policy. One police officer said, "it is very difficult because officers don't know if a particular case is a crime or okay because of the first amendment." Policies thus would help not only SAs, but also police officers who enforce computer crime laws.

There is also a push by Internet activists to have an electronic Bill of Rights. Below is an example of an electronic Bill of Rights with two points most associated with my research topic (see Appendix 8 for complete electronic Bill of Rights):

#3. No body, public or private, shall monitor communication for the purpose of gathering data without the expressed consent of all parties involved in the communication. This includes currently undeveloped technologies, electronic agents, programs, or involuntary disclosure unless authorized by warrant issued by due process of law.

#5. The *Personal Proprietary Information (PPI) of individuals may not be gathered, bought, or traded by any organization without express written or electronic permission, granted by the individual to whom the PPI belongs. The particular information gathered for demographic purposes may not be associated with any individual. Organizations and governmental bodies that do have reason to hold such data must be held responsible for the safe keeping of said data. Said bodies and organizations must annually notify each citizen who has any PPI included in the bodies or organizations data banks exactly what information they maintain and allow the individual a means to alter any incorrect information free of charge.

This electronic Bill of Rights argues that Internet users should be able to control the information that is collected about them.

Similarly, a proposal to allow the user to control cookie information has been recommended by the Internet Engineering Task Force. There is also a privacy rating system proposed by the Electronic Frontier Foundation that would "inform Internet users…the level of privacy they should expect when visiting a site." (Flynn, 1996)

Protecting privacy will also help people control the information gathered about them and thus allow them to prevent the leaking of personal information. Protecting privacy may stop unwanted e-mail advertisements because companies would not be able to sell that information to marketers. Protecting privacy is necessary in the Information Age.

8. CONCLUSION

This research project is exploratory and some aspects of it require further investigation. Are there differences between professional and non-professional SAs? Are there differences in the prevalence of reading a person's e-mail because of the size of the department? What information about users is gathered when they visit a company's website?

Are there two types of SAs? I could not determine this with my data, but, I hypothesize that the two types are, the professional and the non-professional. The professional SA makes a career of such work, whereas the non-professional SA considers the work to be temporary.

The professional SA is a person who understands and should follow his institution's polices. Obviously, this does not happen all of the time and there are always people who violate rules and regulations.

Many professional SAs work under strict guidelines. According to CU's E-mail policy, if any SAs are caught reading someone's e-mail without permission they could be terminated. Most of the SAs I interviewed believe that no one should be able to view an e-mail unless it is sent to them. The farther removed from e-mail duties, the better.

The non-professional SA is someone who does not view this as a career. For example, in one class, students are allowed "superuser" access and must sign a waiver form that they will not read people's e-mail. Moreover, the department this class is taught in has strict rules regarding SA's reading people's e-mail, partly because the person in charge is a major advocate for privacy on the Web.

System administrators were the primary focus of my thesis in the beginning. My

initial thesis topic was, “How often do SAs at CU read student, staff, and faculty e-mail for administrative or personal reasons.” Although I have provided some data on this topic, there was not enough to be a whole honor’s thesis. Therefore, I expanded my research to other areas of the Internet and at the same time narrowed my research to Internet privacy.

Internet privacy exists because of laws, policies, and normative behavior. But laws and policies are “lagging” behind the technology. Ogburn would argue that cultural lag is evident with the people who are supposed to uphold policies and laws, but do not know how to interpret the policies. For the most part, this occurs because the policies are too broad. Ogburn would explain that policies are broad because the people who created the policies do not know the specific issues they may face in the future. Thus policy makers and enforcers have a “wait and see attitude.” Another reason is that police officers may not know the technology very well. (Interview) Moreover, 26% of my sample said they would do nothing if they saw an e-mail account still logged in. Probably, the most courteous thing to do is to log the person out. Internet technology is rapidly evolving and thus, a “cultural lag” exists.

Goffman would argue that it is not the policies and laws that are “lagging”, rather, the people who uphold the policies and laws are in continual “impression management” and want to make sure they do not over step their bounds. Moreover, SAs may want to give the impression that they are following institutional policies; but, in reality read other users’ e-mail messages.

Moreover, e-mail communication seem to bring out the user’s back stage role. Sending an e-mail that is verbally abusive is generally easier than confronting a person

face to face because of the impersonal nature of the communication. Users do not need to "present themselves to others in ways that are most favorable to their own interests or image" because they are communicating with a terminal instead of a person. Thus, a person's back stage becomes the front stage.

Even though there are laws and policies that protect privacy, breaches of privacy occur because of Internet technology. Forwarding an e-mail message could potentially be a breach of privacy if the original author is unaware that his message has been sent to an e-mail list. Cookies provide information on web visitors that could potentially be sold. The last command will show where and when a user has logged in. This could potentially be used as a tracking device because the last command gives the exact location of a user.

Furthermore, privacy breaches are justified because of numerous reasons. Hackers search for fun and challenge by breaking into computer systems and possibly resulting in a violation of a user's privacy. System administrators may have to read an e-mail message in order to redirect the message to its rightful recipient. Companies may gather information about users in order to send e-mail advertisements to them. Although briefly mentioned, variations of policies and laws may affect how SAs, managers, and police officers handle Internet cases and thus should be further researched. The definitions of privacy can be different in each city, state, and country. Therefore different policies and laws will have different meanings and can lead to confusion.

Protecting privacy then fall upon the users, technology and legislation. Users of the Internet need to take more responsibility: understanding what laws and policies

exist that protects their cyber-rights; to an extent learning the technology in order to protect themselves from making mistakes; and users should be allowed to control the information that is gathered about them.

The first step is to be aware of the consequences that new technologies bring. Then people can decide for themselves (instead of having large corporations and institutions decide) what information should be gathered. Moreover, people can then make more informed decisions if the information gathered is detrimental, or pertinent enough to act upon. For example, if a web site obtains the name and phone number of a web visitor, is this important enough to protect? Where do people, institutions, and corporations cross the gray line? Can there be privacy in a communication's medium created to provide information?

Technology can provide protection of privacy. E-mail encryption programs allow users to send messages that hide the content of their e-mail messages. Future web browsers will allow users to control the cookie information. Although encryption programs are difficult to use, hopefully the programs will become more user friendly in the future.

Lastly, legislation is another solution to protect Internet privacy. Laws should provide a guideline on what privacy invasions can and cannot be done. For example, counting how many times a user visits a web site is probably not that harmful; but, obtaining identifiable information like names, and phone numbers should be disallowed. Policies and laws need to be specific about what privacy invasions are allowed and disallowed.

Privacy is protected in many ways over the Internet. Policies, laws, and norms

offer some form of privacy protection. But, the very nature of the Internet does not favor privacy. The Internet was made to communicate information in times of military emergencies, like a nuclear war. It was not created for high level security or keeping information away from other people.

Many findings in my research suggest that the Internet is a communications medium that could allow extensive surveillance. Could the Internet become a "panopticon" of continuous surveillance?

Internet privacy can increase, stay the same, or decrease. If Internet privacy stays the same then much of the invasions of privacy outlined in this paper will remain. Hopefully, the Internet will move toward increased privacy for users because privacy will protect users from unwanted e-mail advertisements, being "followed" on the Internet, and information gathered about them. Although the Internet is not a medium that is conducive to privacy, privacy rights need to be established and protected. Herein lies the challenge and difficulty of the Information Age.

Appendix 1 - Contact E-mail

Dear System Administrator;

I am a Sociology student working on my Honor's thesis and was wondering if I could speak/interview you. I am working closely with Professor Gary Marx and I have already spoken with other SAs and they recommended to me that you would be an excellent source regarding my research topic (e-mail).

I have written a paper on Internet Deviance and if you wish I can send it to you as an attachment.

Please contact me at the below information if you have any questions. I understand that you're an extremely busy person and I appreciate all your help.

Sincerely,

John Wong

Appendix 2 - Interview Agenda

1. Can you please state your title and a short description of it
2. Ask about policy that SAs must go through to get approval to read e-mail of others
3. Can I get a copy of the policy
4. How many times does this often
5. What are legitimate reasons to look at people's email
6. What if a student dies…what happens to the content of the account and email messages
7. Consequences if policy is broken
8. Has anybody been fired
9. Mention story
10. Is it plausible that a SA could read somebody else's e-mail without your office knowing
11. What are the reasons that enable your office to punish a student, faculty or staff member.
12. Have you ever punished a faculty member?
13. Staff or students?
14. Has your office ever called the police or FBI because of what a person did; as a result has anybody been prosecuted before?

Appendix 3 - Survey

General Information

1. Are you male or female?_____

2. Please circle your class ranking.

   Freshman Sophomore Junior Senior Graduate Student

3a. What college or school are you in?_____

3b. What is your major(s)?_____

4. What is your age?_____

5. Can you please circle the ethnic group that you are most associated with?

   African-American Caucasian Native American

   Asian-American Hispanic Other_____

6. Can you please circle the highest educational level of your mother or the person you consider to be your mother?

   No High School Some High School High School or GED Some College

   College Graduate School Other (please specify)_____

7. Can you please circle the highest educational level of your father or the person you consider to be your father?

   No High School Some High School High School or GED Some College

   College Graduate School Other (please specify)_____

8. What kind of work does your mother or the person you consider to be your mother

   do?_____

9. What kind of work does your father or the person you consider to be your father

   do?_____

10. What religion were you raised in?

Protestant Catholic Judaism Atheism None

Buddhism Hinduism Other (please specify)_____

11. Do you consider yourself to be…

Radical Left Liberal Moderate Conservative Radical Right

12. In the recent presidential election which candidate did you favor?

Ross Perot Bill Clinton Bob Dole Ralph Nader

None Other_____

As you fill this survey out, please keep in mind that this is focusing primarily on Electronic Mail and not any other aspect of the Internet.

1. How many times do you use or check Electronic Mail (E-Mail) a day?
   a. None b. 1 to 4 c. 5 to 9 d. 10-14 e. 15+ f. Occasional

2. I have a feeling that there are 3 types of usage for E-Mail, can you please rate from 1 to 10, 1 being the lowest, and 10 being the highest ,what you use E-Mail for?

   - Personal (e.g. friends, family, etc.) - _____
   - Academic (e.g. class list, professor, etc.) - _____
   - Professional (e.g. job, student organization, etc.) - _____
   - Other (e.g. anything else not categorized above) - _____

3a. CU-Boulder constructed an E-Mail policy last Spring. Have you viewed this document before?

Yes No

3b. If you did read it, then how much?

All of it Some of it Heard about it

Please circle the appropriate response to the following scenarios about E-Mail and the Internet.

4. A student passes away and her parents want to view the content of her E-Mail account, all of her new messages and all of the E-Mail she has ever sent. Do you believe that parents should have this right?

Definite Yes Yes Undecided No Definite No

5. If a SA (a person who makes sure that E-Mail machines run smoothly) runs across an E-Mail message with the statement "I'm going to kill you," Should the SA report this to his/her superiors or the police?

Definite Yes Yes Undecided No Definite No

6. You walk by a computer and notice that another person has left his/her E-Mail account logged in. Of the below examples, which of the following resembles the one you will more likely do?

Log the person out Take a peek at his/her files Nothing Start deleting stuff

Play a joke Use his/her E-Mail Other (please specify)_____

7a. When you write an E-Mail message, what do you think are the chances of a third party reading it?

Likely Impossible Not Likely

7b. Are you worried about this?

Yes Slightly worried Not at all

8. Should CU-Boulder ban access to pornographic web sites from campus computer labs?

Definite Yes Yes Undecided No Definite No

9. Should CU-Boulder ban access to White Supremacist web sites from campus computer labs?

Definite Yes Yes Undecided No Definite No

10. If you were to receive fifty E-Mail messages a in day, which of the following best describes your reaction?

Annoyance Pleasure Pick out the important ones Ignore messages

11. Are there important issues that have not been discussed earlier regarding E-Mail and the Internet?

Yes No

12. If Yes, what are they?

Appendix 4 - Colorado Computer Crime Statute

18-5.5-102. Computer crime.

(1) Any person who knowingly uses any computer, computer system, computer network, or any part thereof for the purpose of devising or executing any scheme or artifice to defraud; obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises; using the property or services of another without authorization; or committing theft commits computer crime.

(2) Any person who knowingly and without authorization uses, alters, damages, or destroys any computer, computer system, or computer network described in section 18-5.5-101 or any computer software, program, documentation, or data contained in such computer, computer system, or computer network commits computer crime.

(3) If the loss, damage, or thing of value taken in violation of this section is less than one hundred dollars, computer crimes is a class 3 demeanor; if one hundred dollars or more but less than four hundred dollars, computer crime is a class 2 misdemeanor; if four hundred dollars or more but less than fifteen thousand dollars, computer crime is a class 5 felony; if fifteen thousand dollars or more, computer crime is a class 3 felony.

Appendix 5 "E-Mail" Policy

Electronic mail has become an essential tool for faculty, staff, and students of the University. Yet like all powerful tools, it has the ability to damage as well as to assist. In 1993, the Policy Board for Information Technology asked the assistant vice president for computing and information systems to draft a University e-mail policy to promote constructive, rather than destructive, use of e-mail. A working group including representatives of information technology, internal audit, legal counsel, personnel, and faculty prepared the policy after reviewing comparable documents from around the country.

The policy addresses issues of privacy and responsible use. It defines permissible and prohibited use and gives examples. It states the University's right to access and disclose the contents of electronic communications, but also sets forth the requirements for prior approval of such access.

After extensive review on all the campuses, the following statement has been adopted as an official administrative policy statement of the University. If you have questions about the policy, contact Lindsay Winsor at University Management Systems Winsor_l@wizard.Colorado.EDU.

I. Introduction

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) that made it illegal to intercept electronic communications on a public or private network without proper authorization. The ECPA provides electronic transmission of messages the same privacy protection as telephone calls over the public telephone systems. System operators of public networks are not permitted to divulge the contents of messages except under a narrow set of circumstances.

The ECPA also protects internal systems, such as those at the University of Colorado, from unauthorized interception of messages by outside sources. However, the ECPA permits messages that are stored on internal systems to be accessed by authorized personnel without violating the Act.

This statement sets forth the University's policy with regard to use of, access to, and disclosure of electronic communications. For purposes of this policy statement, electronic communications includes but is not limited to electronic mail, Internet services, voice mail, audio and video conferencing, and facsimile messages that are sent or received by faculty, staff, students, and other authorized users of University resources. Attached to the statement are two appendices: one providing concepts for consideration in granting approval to access electronic communications of others, and one discussing e-mail privacy and ethics.

Author's Note: This can be viewed at the following web address:
http://www.Colorado.EDU/HyperHelp/news-info/email.html

II. Policy

A. Permissible Uses of Electronic Communications

1. Purpose of Use - The use of any University resources for electronic communications should be related to University business including academic pursuits.

2. Authorized Persons - Only faculty, staff, students, and other authorized persons conducting University business may use the electronic communication systems.

B. Prohibited Uses

1. Personal, Commercial Purposes - University resources for electronic communication shall not be used for personal, commercial purposes. Incidental and occasional personal use of electronic mail and voice mail may occur when such use does not generate a direct cost for the University, but such messages will be treated no differently from other messages. (An example of a use that does not create a direct cost is placing a local telephone call: the University will pay no more for telephone service than it would have paid had the call not been made. An example of a use that does create a direct cost is placing a long-distance telephone call: the University will pay a direct charge for that call. Likewise, any activity that involves printing creates a direct cost.)

2. Other Prohibited Use - Other prohibited electronic communications include, but are not limited to:

   a. Use of electronic communications to send copies of documents in violation of copyright laws.

   b. Use of electronic communication systems to send messages, access to which is restricted by laws or regulations.

   c. Capture and "opening" of undeliverable electronic communication except as required in order for authorized employees to diagnose and correct delivery problems.

   d. Use of electronic communications to intimidate others or to interfere with the ability of others to conduct University business.

   e. "Spoofing," i.e., constructing electronic communication so it appears to be from someone else.

   f. "Snooping," i.e., obtaining access to the files or communications of others for the purpose of satisfying idle curiosity, with no substantial University business purpose.

g. Attempting unauthorized access to data or attempting to breach any security measures on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.

C. University Access and Disclosure

1. Grounds Required for Access - The University reserves the right to access and disclose the contents of faculty, staff, student, and other authorized users' electronic communications, but will do so only when it has a legitimate business need such as those listed in number 2 below, and only with explicit authorization. The University's electronic communication systems should be treated like a shared filing system-i.e., with the expectation that messages sent or received on University business or with the use of University resources may be made available for review by any authorized University official for purposes related to University business.

2. Monitoring of Messages - The University will not monitor electronic messages as a routine matter.

   The University will inspect the contents of electronic messages in the course of an investigation triggered by indications of misconduct, as needed to protect health and safety, as needed to prevent interference with the academic mission of the institution, or as needed to locate substantive information required for University business that is not more readily available by some other means. The University will respond to legal processes and fulfill its obligations to third parties.

3. Limitations on Disclosure and Use of Information Obtained by Means of Access or Monitoring - The contents of electronic communications, properly obtained for legitimate business purposes, may be disclosed without permission of the employee. The University will attempt to refrain from disclosure of particular messages if disclosure could create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

4. Special Procedures to Approve Access, Disclosure or Use of Electronic Messages - Individuals needing to access the electronic communication of others, to use information gained from such access, and/or to disclose information from such access must obtain approval for such activity in advance. The chancellor of each campus shall develop a written statement of procedure to be followed to request such approval. That procedure shall take into consideration ways to minimize the time and effort required to submit and respond to requests, the need to minimize interference with University business, and the rights of individuals.

D. Disciplinary Action

Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of the University's electronic communications resources.

Attachment I: Concepts for Granting Approval to Access Electronic Communications of Others

The following are suggestions for elements to be considered in designing the process for granting approval to access electronic communications addressed to others:

1. What information is needed to determine whether a request should be approved? Possibilities include:
   - Name and title of the person whose communications will be accessed;
   - Name and title of the person who will do the accessing;
   - Why the access is needed;
   - What forms of communication will be accessed (e.g., voice mail, e-mail, FAX);
   - Required duration of the access;
   - What will be done with the accessed messages? With whom will they be shared?

2. Who should be able to request access? Who should be able to approve requests? Possibilities include:
   - Department chairpersons and unit directors should be able to request access;
   - Deans or vice chancellors should be able to approve requests.

3. Who needs to be informed when a request is approved to implement the access? The approved request must be routed to those people who should keep a copy of the request.

4. What advice or reminders should be given to the person requesting the access? Possibilities include:

   - A reminder that concerns about fiscal misconduct or criminal activity should not be investigated by individuals or departments but should be referred to University police or internal audit staff in accordance with the University administrative policy titled "Reporting Fiscal Misconduct."

   - A reminder that the contents of electronic communications obtained after appropriate authorization may be disclosed without the permission of the employee. At the same time, the University will attempt to refrain from disclosure of particular messages if disclosure could create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

Attachment II: Statement on E-mail Privacy and Ethics

Electronic mail, or e-mail, is a very useful tool for doing your University work. But you need to understand the nature of e-mail and use it wisely to avoid unpleasant consequences. Please read the following facts and tips about e-mail before you send your next e-mail message.

I. Privacy

A. The Facts of E-mail Privacy - E-mail is not exactly like a phone call. More information, including copies of the content of your messages, is routinely recorded about your use of e-mail than about your use of the telephone. Moreover, a broader, less controlled set of people have access to that information. E-mail is not like a letter in an envelope. The contents of your message are out in the open, and there's no easy way to mark a message "confidential." E-mail is most like a postcard. The contents of your message may be viewed during the mailing process. If it is inadequately addressed, or if there is a problem with routing equipment, a "postmaster" may read your message to try to redirect it correctly. Your message may be delivered to the wrong address. Your message can be forwarded or printed. Your message will probably be stored, perhaps in your directories, perhaps in the directories of the person who receives the message, and probably on system back-up tapes, which may be retained for very long periods of time.

   We suggest you keep this "picture" of e-mail in mind as you compose e-mail messages. Don't put anything in an e-mail message that you wouldn't want posted on a bulletin board or used in a lawsuit or shared with the wrong person. Do use professional, courteous language that will not embarrass you later. People who may never meet you will be forming impressions about you based on the way you compose your e-mail messages. It's much easier to edit a message before you send it than to send an apology later. If you receive mail that obviously was not intended for you, send a reply to the sender notifying them that they need to revise the address.

   The technology of the University's e-mail systems is constantly being upgraded. Over time, the technical ability to ensure privacy of e-mail communication will increase. But it is best to assume that e-mail is a public medium and to avoid using it for confidential communication.

B. The Policy of the University: The University has formally adopted a policy regarding use of the University's electronic communications resources, which includes electronic mail. You need to be aware of this policy as you use any of the electronic communications resources.

II. Ethics

The University's e-mail systems are developed and maintained to accomplish the work of the University. You should use them for academic pursuits and University- related administrative tasks, abiding by all applicable guidelines and policies. Naturally, you may want to use e-mail for personal communication that is not directly related to your role at the University. A minimal amount of such use is acceptable. Use good judgment and limit the amount and frequency of such use. Never use University e-mail systems for personal gain. Help conserve e-mail resources. If you flood the system with trivia, it won't be available for other more worthwhile uses. Never send junk mail, random mail, or "Who are you?" messages.

Limit your use of lists as much as possible: Many of the global e-mail lists are available in other forms, Network News, Gopher, etc., and using those other means of accessing lists will require fewer computer resources than subscribing to a list. If you subscribe to a list, always make sure that you know how to unsubscribe from that list, and do so when you no longer have a use for the information from the list, or when you are ready to stop using e-mail at the University. Be careful when sending to e-mail lists. Sending large messages to lists that may have hundreds of users can dramatically impact both the e-mail system you are using to send the message and the e-mail systems receiving the message. Before sending to any list or replying to any message from a list, make sure that you know the guidelines and policies of that list and that you are aware of where your message is going (to the whole list, or just the person that sent the original message).

Let integrity and honesty guide your use of e-mail and it will be an effective, useful tool for your work at the University.

Appendix 6 - "Responsibility of Users" Policy

The use of computing and networking resources at the University of Colorado at Boulder is a privilege, and, like any other privilege, carries with it the responsibility for making use of these resources in an efficient, ethical, and legal manner. Computing and Network Services depends upon the spirit of mutual respect and cooperative attitudes to ensure that everyone has equal privileges, privacy, and protection from interference or harassment. The systems shall be used in a manner consistent with the instructional, research, and administrative objectives of the University community in general and with the purpose for which such use was intended. All activities inconsistent with these objectives are considered to be inappropriate and may jeopardize continued use of computing facilities and networks. Computing and Network Services reserves the right to examine users' stored information when investigating cases of computing abuse; in addition, it may withdraw computing privileges when violations have occurred.

As a condition of use of Computing and Network Services facilities, the user agrees:

- To respect the stated purpose of accounts on the systems. Individuals shall use accounts only for the purposes specified and shall not use any other individual's account unless explicitly permitted to do so by the person authorized to use that account. Users should not share their personal account passwords with friends or classmates. Users are responsible for any activity conducted on their personal accounts. Under no circumstances shall CNS resources (computers, software, networks, printers, plotters, scanners, etc.) be used for personal financial gain.

- To respect the privacy of other users. Users shall not intentionally seek information on, obtain copies of, or modify files, tapes, passwords or any type of data belonging to other users unless specifically authorized to do so. Electronic mail shall not be used to harass other users. Nor may users create, send, or forward e-mail chain letters (e-mail that requests that it be forwarded to other people). Attempts to alter the "From:" line or other attribution of origin in electronic mail will be considered transgressions of University rules.

- To respect the integrity of the systems. Individuals shall not use CNS resources to develop or execute programs that could harass other users, infiltrate the systems, or damage or alter the software components of the systems.

- To respect the resource controls of the systems. Users shall not attempt to alter or avoid accounting for computing services. Users should avoid excessive use of resources, controlled or otherwise. For example, personal computers, dial-in lines, graphics devices, printers, mainframe processor time, and data networks are resources that must be shared in an equitable manner.

Author's Note: This policy can be viewed at the following web address:
http://www.colorado.edu/CNS/docs/responsibilities.html

- To respect the privileges of network connectivity. Membership in the wider community of network users carries with it responsibility for ethical conduct similar to what is required on UCB systems. Users should avoid harassing other users, violating others' privacy, tampering with security provisions, or attempting entry to non-public hosts. They should be mindful that they are often guests on other institutions' hosts.

- Ethically responsible use of computing systems includes the efficient and productive use of the resources. For example, users must not tie up resources through game playing or other trivial applications; sending frivolous or excessive mail, including chain mail; or printing excessive copies of documents, files, images, or data. Keeping unnecessarily large files on shared systems also causes the unnecessary depletion of resources.

Software programs are protected by Section 117 of the 1976 Copyright Act. Unless they have written the program themselves, users do not have the right to make and distribute copies of programs without specific permission of the copyright holder.

Violations of these conditions may result in the suspension of computing privileges; disciplinary review, which may include suspension or expulsion from the University; termination of employment; or legal action.

The physical abuse of any computing equipment or supplies will be reported to the University Police and to the appropriate administrative office. Student offenders will also be reported to the Office of Judicial Affairs.

Any instance of academic dishonesty--for example, using other people's files or gaining access to instructors' files--will be reported to the student's professor and to the associate dean of the student's college or school, as well as to the Office of Judicial Affairs

Appendix 7 - Consent form to read e-mail

Concepts and Template for Granting Approval to Access Electronic Communications of Others

The following are suggestions for elements to be considered in designing the process for granting approval to access electronic communications addressed to others:

1. What information is needed to determine whether a request should be approved? Possibilities include:

    * Name and title of the person whose communications will be accessed;
    * Name and title of the person who will do the accessing;
    * Why the access is needed;
    * What forms of communication will be accessed (e.g., voice mail, E-Mail, FAX);
    * Required duration of the access;
    * What will be done with the accessed messages? With whom will they be shared?

2. Who should be able to request access? Who should be able to approve requests? Possibilities include:

    * Department Chairpersons and Unit Directors should be able to request access;
    * Deans, or Vice Chancellors should be able to approve requests.

3. Who needs to be informed when a request is approved to implement the access? The approved request must be routed to those people who should keep a copy of the request

4. What advice or reminders should be given to the person requesting the access? Possibilities include:

    * A reminder that concerns about fiscal misconduct or criminal activity should not be investigated by individuals or departments but should be referred to University Police or Internal Audit staff in accordance with the University Administrative Policy titled "Reporting Fiscal Misconduct".

    * A reminder that the contents of electronic communications obtained after appropriate authorization may be disclosed without the permission of the employee. At the same time, the University will attempt to refrain from disclosure of particular messages if disclosure could create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

A sample access request form is attached.

REQUEST TO ACCESS ELECTRONIC COMMUNICATIONS OF OTHERS

Our department requests authority to access electronic communications sent to an individual as described below:

1. Name, Title, and Department of person whose communications would be accessed:

   _____ _____
   Name Title

   _____
   Department

2. Name, Title, and Department of person who will do the accessing:

   _____ _____
   Name Title

   _____
   Department

3. Reason for access request:_____

   _____

   _____

4. What forms of communication will be accessed (e.g., voice mail, E-Mail, FAX) _____

   _____

5. How long should the special access last? _____

6. What will be done with the accessed messages? With whom will they be shared? _____

   _____

   _____

7. _____ _____
   Signature of Requesting Department Chairperson or Unit Director Date

8. _____ _____
   Signature of Approving Dean or Vice Chancellor Date

9. Upon approval, this form is to be delivered to the following person as authorization for them to implement the requested special access.

   _____ _____
   Name Title

   _____
   Department

Appendix 8 - Electronic Bill of Rights

Last revised: March 8, 1997

Developed by the Electronic Frontiers Florida

Preliminary Statement:

The People of the United States, in Order to Secure their Rights in the Electronic Frontier into the Twenty-first Century and Beyond, Hereby Proclaim These to Be Fundamental Rights in Cyberspace. As Personal Privacy, Security and Freedom of Speech and Information are already guaranteed to the citizens of the United States of America, we once again Lay Claim to these Rights, Without Exception, and Extend the Current Standards to Include what is Commonly Known as Cyberspace.

#1. There shall be no law that censors any data transmission that does not apply to printed media.

#2. The various means of security available to the people are necessary for the overall continuance of a free State. The right of the people to utilize encryption, passwords, passphrases and firewalls free of mandatory disclosure or escrow of private keys, or key recovery agents by any name or in any form shall not be infringed upon. Also any individual, organization or company has the right to develop and distribute encryption algorithms capable of producing any key length or source code via electronic media.

#3. No body, public or private, shall monitor communication for the purpose of gathering data without the expressed consent of all parties involved in the communication. This includes currently undeveloped technologies, electronic agents, programs, or involuntary disclosure unless authorized by warrant issued by due process of law.

#4. The ability to detect the integrity of communications by the intended recipient and the initial sender shall not be violated, restricted or infringed upon. Likewise, there shall be privacy in both material effects and data transmissions.

#5. The *Personal Proprietary Information (PPI) of individuals may not be gathered, bought, or traded by any organization without express written or electronic permission, granted by the individual to whom the PPI belongs. The particular information gathered for demographic purposes may not be associated with any individual. Organizations and governmental bodies that do have reason to hold such data must be held responsible for the safe keeping of said data. Said bodies and organizations must annually notify each citizen who has any PPI included in the bodies or organizations data banks exactly what information they maintain and allow the individual a means to alter any incorrect information free of charge.

#6. In the interest of free and unfettered speech there shall be no law mandating that the identity of a person be associated with one's identity while communicating via any on line environment, platform or protocol. The only scenario in which an on-line service provider shall be free to divulge this information to any organization without the expressed, documented permission of the individual concerned is in the event that the service provider has been served with a legally warranted demand.

#7. All public records must be made openly available in a free and timely manner via electronic transmission. In the case of PPI, the government must maintain a set of standards to ensure the security of this information in that the individual requesting access to the information is indeed the individual to whom it belongs.

#8. There shall be established a new standard for classification of PPI held by a government body or agency, and/or any organization or company which will fall between the already established standards of governmental classified information and sensitive information.

#9. All public schools, universities and libraries shall have devices maintained for the sole purpose of accessing the GII.

BIBLIOGRAPHY

Barlow, John-Perry. 1991. "Fear and Loathing in San Francisco." *Index on Censorship*; 1991, 20(7) July, 27-30.

Barnes, Douglas. 1994. "The Coming Jurisdictional Swamp of Global Internetworking." www.communities.com/papers/swamp.html. Nov. 16, 1994.

Batty, Michael; Barr, Bob. 1994. "The Electronic Frontier. Exploring and Mapping Cyberspace." *Futures*; 1994, 26(7) Sept., 699-712.

Behar, Joseph. 1993. "Computer Ethics: Moral Philosophy or Professional Propaganda?" *Computers in Human Services*; 1993, 9(3-4) 441-453.

Berman, Bruce. 1989. "The Computer Metaphor Bureaucratizing the Mind." *Science as Culture*; 1989, 7, 7-42.

Beeson, Ann. 1996. "Privacy in Cyberspace: Is your E-mail Safe From the Boss, the SysOp, the Hackers, and the Cops?" Published on American Civil Liberties Union website: www.aclu.org. July 1, 1996.

Borella, Michael. 1992. "Computer Privacy vs. First and Fourth Amendment Rights." Electronic Frontier Foundation website: www.eff.org.

Caruso, Denise. 1996. "FTC to Study Internet Privacy." *New York Times* website: www.nytimes.com. June 3, 1996.

Clough, Bryan; and Mungo, Paul. 1992 Approaching Zero. NY: Random House.

Collier, P.A.; Spaul, B. J. 1992. "Problems in Policing Computer Crime." *Policing and Society*; 1992, 2(4) 307-320.

Computer Professional for Social Responsibility. "Electronic Privacy Guidelines." www.cpsr.org.

Conference on World Affairs. 1996. Open and Closed: Bullies, Hackers and Saints - The Internet Changes it All. April 12. Roger Ebert, Burgess Laird, Oliver McBryan, Ulrich Trottenberg, and Phillip Zimmerman were the panelists.

Cunningham, Scott; Porter, Alan. 1992. Communication Networks: A Dozen Ways They'll Change our Lives. Futurist; 1992, 26, 1, Jan-Feb, 19-22.

Cyberspace Law for Non-Lawyers. "Privacy Law in Cyberspace." www.counsel.com.

Authors Note: The bibliography consists of works that I used as references as well as works that I directly cite.

Duranti, Alessandro. 1986. Framing Discourse in a New Medium: Openings in Electronic Mail. *Quarterly Newsletter of the Laboratory of Comparative Human Cognition*; 1986, 8, 2, Apr., 64-71.

Fitch, Malcolm. 1997. "Here's how to protect your wallet (and your privacy) from online pirates." *Money*. April 1997, p. 32.

Flynn, Laurie. 1996. "Group to Monitor Web Sites For Respect of Consumer Privacy." *New York Times* website: www.nytimes.com. July 16, 1996.

Forester, Tom; and Morrison, Perry. 1990. "Computer Crime: New Problem for the Information Society." *Prometheus*; 1990, 8(2) Dec., 257-272.

Glave, James. 1997. "Next Netscape Will Chew Cookies on Command." *Wired News* website: www.wired.com. Feb. 22, 1997.

Gerson, Elihu M. 1988. "Electronic Mail." *Qualitative Sociology*; 1988, 11(4) Winter, 355-358.

Graber, Doris. 1995. "Potholes along America's Public Information Superhighway." *Research in Political Sociology*; 1995, 7, 299-324.

Harper, R.-R. 1991. "The Computer Game: Detectives, Suspects, and Technology." *British Journal of Criminology*; 1991, 31(3) Summer, 292-307.

Hawn, Matthew. 1997. "Easy Now to Keep Tabs on Users' Internet Postings." *New York Times* website: www.nytimes.com. January, 6, 1997.

Hollinger, Richard. 1993. "Crime by Computer: Correlates of Software piracy and Unauthorized Account Access." *Security Journal*; 1993, 4(1) Jan., 2-12.

Johnson, David. 1994. "The Unscrupulous Diner's Dilemma and Anonymity in Cyberspace." Electronic Frontier Foundation website - www.eff.org. March 4, 1994.

_____ 1994. "Electronic Communications Privacy: Good Sysops Should Build Good Fences." Electronic Frontier Foundation website - www.eff.org. 1994.

Junnarkar, Sandeep. 1997. "Medical Records are Headed to the Internet." *New York Times* website: www.nytimes.com. February 15, 1997.

Kapor, Mitchell. 1991. "Civil Liberties in Cyberspace: When does hacking turn from an exercise of civil liberties into crime?" *Scientific American*, Sept. 1991.

Katz, James; and Tassone, Annette. 1990. "Public Opinion Trends: Privacy and Information Technology." *Public-Opinion-Quarterly*; 1990, 54(1) Spring, 125-143.

Kendall, Diana. 1996. Sociology In Our Times. Wadsworth Publishing Company.

Klass, Tim. 1997. "New Security Flaw Found in Microsoft Internet Browser." *New York Times* website: www.nytimes.com. March 8, 1997.

Kling, Rob; and Iacono, Suzanne. 1984. "Computing as an Occasion for Social Control." *Journal of Social Issues*; 1984, 40(3) Fall, 77-96.

Landreth, Bill. 1985. Out of the Inner Circle - A Hackers Guide to Computer Security. Bellvue, WA: Microsoft press.

Littman, Jonathan. 1996. The Fugitive Game. NY: Little, Brown, and Company.

Lyon, David. 1993. "An Electronic Panopticon? A Sociological Critique of Surveillance Theory." *Sociological Review*; 1993, 41(4) Nov., 653-678.

Madusda, Yoneji. 1979. "Privacy in the Future of Information Society." *Computer Networks*; 1979, 3(3) June, 164-170.

Marcoulides, George. 1991. "An Examination of Cross-Cultural Differences toward Computers." *Computers in Human Behavior*; 1991, 7(4) 281-289.

Markoff, John. 1996. "Voluntary Rules Proposed to Help Insure Privacy for Internet Users." *New York Times* website: www.nytimes.com. June, 5, 1996.

_____ 1996. "Balancing Privacy and Official Eavesdropping." *New York Times* website: www.nytimes.com. July, 13, 1996.

_____ 1995. "A Most-Wanted Cyberthief Is Caught in His Own Web." New York Times website: www.nytimes.com. February 16, 1995.

Marien, Michael. 1997. "Top Ten Reasons the Information Revolution is Bad for Us." *Futurist*. Jan.-Feb. 1997.

Marx, Gary. 1994. "New Telecommunications technologies require new manners." *Telecommunications Policy* 18, 538-551.

_____ 1991. "The New Surveillance." *National Forum*; 1991, 71(3) Summer, 32-36.

_____ 1990. "Privacy and Technology." *The World and I*; September 1990.

_____ 1988. Undercover. Berkeley: University of California Press.

Matheson, Kimberly; and Zanna, Mark. 1988. "The Impact of Computer-Mediated Communication on Self-Awareness." *Computers in Human Services*; 1988, 4(3) 221-233.

Michalowski, Raymond; and Pfuhl, Erdwin. 1991. "Technology, Property, and Law: The Case of Computer Crime." *Crime, Law and Social Change*; 1991, 15(3) May, 255-275.

McKeown, Patrick. 1992. "Computer Crimes and Criminals." *National Forum*; 1992, 72(3) Summer, 46-47.

Morley, Mark. 1993. "The Supreme Court and Electronic Surveillance: A study of Originalism, the Fourth Amendment, and the Powers of Law Enforcement." Electronic Foundation Frontiers website - www.eff.org. Dec. 21, 1993.

Myers, David. 1987. "Anonymity is Part of the Magic: Individual Manipulation of Computer Mediated Communication Contexts." *Qualitative Sociology*; 1987, 10(3) Fall, 251-266.

National Research Council. 1997. "Pressure Needed to Improve Security and Privacy of Electronic Health Records." www2.nas.edu. March 5, 1997.

Office of Technology Assessment. 1985. Federal Government Information Technology: electronic surveillance and civil liberties. Chapter titled "Electronic Mail Surveillance." Washington D.C.: Congress of the U.S., Office of Technology Assessment.

Parker, Donn. 1976. *Crime by Computer*. NY: Charles Scribner's and Sons.

Perrolle, Judith. 1991. "Computer-Mediated Conversation." *National Forum*; 1991, 71(3) Summer, 21-23.

Pfuhl, Erdwin H. 1987. "Computer Abuse: Problems of Instrumental Control." *Deviant Behavior*, 8: 113-130.

Pocius, Kym. 1991. "Personality Factors in Human-Computer Interaction: A Review of the Literature." *Computers in Human Behavior*; 1991, 7(3) 101-135.

Sassi, Sinikka. 1995. "A Self Willed and Odd Thing called the Net: Remarks on the Quality of the Network World." *Nordicom Review*; 1995, 1, 49-58.

Shields, Robert. 1995. Cultures of Internet. London: Sage Publications.

Shimora, Tsutomu. 1996. Takedown: Pursuit and Capture of Kevin Mitnick. NY: Hyperion.

Slatalla, Michelle; and Quittner, Joshua. 1995. Masters of Deception. NY: HarperCollins.

Smith, Stephen. 1994. "Communication and the Constitution in Cyberspace." *Communication Education*. April 1994.

Spetalnick, Terrie. 1993. "Privacy in the Electronic Community." *Educom*. May/June 1993.

Stanley, Christopher. 1995. "Teenage Kicks: Urban Narratives of Dissent not Deviance." *Crime, Law and Social Change*; 1995, 23(2) 91-119.

Stepanek, Marcia. 1997. "Medical Data Privacy Needs Protection, Panel Says." *Wired News* website: www.wired.com. March 5, 1997.

Straub, Detmar W. 1994. "The Effect of Culture on IT Diffusion: E-Mail and FAX in Japan and the U.S." *Information Systems Research*; 1994, 5(1) Mar, 23-47.

Stutz, Michael. 1997. "Shockwave Security Hole Leaves Email Exposed." *Wired News* website: www.wired.com. March 14, 1997.

Van Duyn, J. 1985. The Human Factor in Computer Crime. NJ: Petrocelli Books.

Walther, Joseph. 1992. "Interpersonal Effects in Computer-Mediated Interaction: A Relational Perspective." *Communication Research*; 1992, 19(1) Feb., 52-90.

Wayner, Peter. 1997. "New Found Security Hole Allows Attackers to Read E-mail and Files." *New York Times* website: www.nytimes.com. March 15, 1997.

Whiteside, Thomas. 1978. Computer Capers. NY: Thomas Y. Crowell, Publishers.

Wong, John. 1996. "Super Highway Robbery: Deviance on the Internet." Paper unpublished.