1997

Privacy issues dealing with technology : a review of the literature

Kimberly S. McCoy
University of Northern Iowa

Privacy issues dealing with technology : a review of the literature

Abstract

The sophisticated applications of technology are expanding everyday. Unfortunately, so are the many concerns individuals in society are having about their right to privacy. The actual regulations dealing with one's right to privacy has not expand as rapidly as the applications of technology. Individuals using various types of technology are under the assumption their activities are private; however, this is not the case. It does not seem to matter if you are using a computer for communications work, school, or in the "privacy" of your own home, there is absolutely no privacy when dealing with this type of technology.

This review of this literature reports on how and why tracking is being conducted, some suggestions on how to protect your cyberspace activities, the laws concerning technology and privacy, and the current debate on encryption technology and the government.

Privacy Issues Dealing With Technology:

A Review of the Literature

A Graduate Research Paper

Submitted to the

Division of Educational Technology

Department of Curriculum and Instruction

in Partial Fulfillment

of the Requirements of the Degree

Master of Arts

UNIVERSITY OF NORTHERN IOWA

by

Kimberly S. McCoy

December 1997

This Review by: Kimberly S. McCoy

Titled: Privacy Issues Dealing With Technology Programs: A Review of the Literature

has been approved as meeting the research requirement for the Degree of Master of Arts.

Sharon E. Smaldino

December 16, 1997
Date Approved

Graduate Faculty Reader

12-16-97
Date Approved

R. Muffoletto

Graduate Faculty Reader

12-16-97
Date Approved

R. Muffoletto

Head, Department of Curriculum and Instruction

TABLE OF CONTENTS

Abstract

The sophisticated applications of technology are expanding everyday. Unfortunately, so are the many concerns individuals in society are having about their right to privacy. The actual regulations dealing with one's right to privacy has not expand as rapidly as the applications of technology. Individuals using various types of technology are under the assumption their activities are private; however, this is not the case. It does not seem to matter if you are using a computer for communications work, school, or in the "privacy" of your own home, there is absolutely no privacy when dealing with this type of technology. This review of this literature reports on how and why tracking is being conducted, some suggestions on how to protect your cyberspace activities, the laws concerning technology and privacy, and the current debate on encryption technology and the government.

CHAPTER ONE

Introduction

Viewing one's transactions is not a difficult task in cyberspace. When electronic transactions occur, they pass through a variety of computer networks before reaching the final destination. According to Miller (1997), interacting on the Internet means no privacy. Not many users in the electronic age realize their technological activities have the possibility of being observed by millions of individuals. Miller argued, "Cyberspace blinks with thousands of electronic eyes that watch your every move, tracking where you're from, where you go, how long you stay" (p.1). Several consumer organizations, such as The Center for Democracy and Technology, and The Electronic Privacy Information Center, make numerous efforts to educate on-line users about the lack of confidentiality in cyberspace. Nonetheless, it is apparent a number of individuals are unaware of the lack of privacy in their cyberspace activities. For several years, privacy issues dealing with technology mainly dealt with government concerns. Miller emphasized, "With the explosive growth of the Internet, private sector issues, have become even more serious. . . It's important that some controls be placed on those activities" (p.1). In today's society, tracking and monitoring are accomplished in several different forms. For instance, tracking can be done through the service provider, the company one is working for, the federal government or the vendors one might be interest in.

Purpose

Adequate privacy protection is necessary in order for technology to grow successfully (Rotenberg, 1992). As Besson (1996) stated, "The same technology that promotes the First Amendment values of free speech, association, and access to information also poses a serious threat to another fundamental constitutional value - the right to privacy" (pg. 1). For at least four years, The United States has been debating privacy protection in the electronic age. Rotenberg confirmed, "In the absence of a coherent federal policy to protect privacy, consumers have been left to fend for themselves,

and the response is not encouraging" (p.2). It is the responsibility of the Federal Government to provide rules and regulations appropriate and adequate for dealing with a person's cyberspace activity (Wiesner, cited in Rotenberg, 1992). So few people actually realize how easy it is for one to track and monitor their Internet activities. For example, Federal Law states (cited in Privacy In Cyberspace, 1995-97), "It is not illegal for anyone to view or disclose an electronic communication if the communication is "readily accessible" to the public" (Electronic Communications Privacy Act, 18 U.S.C. 2511(2)(g)(i)).

Before addressing the purpose of this literature review, some key terms will be defined. A web browser is a program that is used to view documentation on the Internet (Plymouth State College, 1996). Network Solutions, Inc (1996) defined a web search engine as:

> A interactive tool to help people locate information available via the World Wide Web. A web search engine is actually a database that contain references to thousands of resources. Users are able to interact with the database, submitting queries that "ask" the database, if it contains resources that match specific search terms. (p.1)

Java Script is a language used for developing Internet applications (Ongoing JavaScript Development, 1997). Cheshire Network Services (1996) defined applet, "As a small executable module, that normally doesn't have the complete features and user interface of a normal application" (p.1).

Netscape Communications Corporation (1997) defined cookies:

> Cookies help Web sites maintain user states. This means that Web sites can "remember" information about users to facilitate their preferences for a particular site, transparent user passwords, and so forth. More specifically cookies allow Web sites (servers) to deliver simple data to a client (user); request that the client store the information; and, in certain circumstances, return the information to the Web site. (p.1)

A chat room is an existing channel. This channel has a group of individuals that receive some type of information or message that is sent to a particular channel. The channel is referred to as the chat room or the location of the chat room. In order to log-on, the user has to address a particular topic or channel they wish to enter. The user can also enter into more than one room at the same time; however, the maximum amount of rooms the user can enter depends on the Chat Server that the user is connected to (What Is a Chat Room?, 1997).

The right to privacy is extremely important when dealing with the role technology has played and will continue to play in the 21st century. The question becomes how has the rapid growth of technology increased the privacy concerns with one's right to privacy in the government arena, private sector, higher institutions of learning and the general public? The purpose of this paper is to review the issues dealing with privacy and technology, take a closer look at encryption technology, and discuss the current statues of privacy laws dealing with the Internet.

CHAPTER TWO

Review of the Literature

Monitoring: On-line

Personal information does not mean private when it has to do with the Internet. The electronic age has made collecting personal information simpler than it used to be. When companies and other sites gather personal information, sometimes permission is granted and most of the time no restrictions are given on how this information could be used (Stellin, 1995-97b). Unfortunately, search engines such as Yahoo, Infoseek, Switchboard, and Excite have the capabilities of gathering personal information: name, address, home phone numbers, electronic mail address and home pages. Monier (cited in Stellin, 1995-97b) proclaimed, "Everyone needs to realize that the web is a public forum. People who publish on the web have to understand the meaning of the word publish" (p.5). Switchboard and Yahoo, two of the most popular search engines, offer business and residential information for individuals on-line. However, these two search engines provide guidelines and general information on how to remove your name from the databases. Stellin (1995-97b) stated, "America On-line, CompuServe, and Microsoft Network all sell their subscriber lists to third parties" (p.3). Consumers can request that on-line services do not share their personal information with outside individuals. According to Stellin, the only thing users can do once they find out that their personal information has been shared with other sites and sources on the web is to inform the individuals who monitor the search engine that they would like their personal information removed.

Registrations at different web sites mean those web sites have the opportunity to collect and store personal information about the individuals who visit the site. This allows them to "personalize" and tailor to the user's wants and needs; however, these web sites do not inform the user how this information might be used (Stellin, 1995-97b). Stellin stated, "There are no regulations that govern the use of information collected by web sites" (p.1).

Personalized services provide chances for the browser to bookmark the sites they visit on a regular basic; however, by creating and leaving the bookmark, the user is allowing others ample opportunity to enter into their "so- called" personal space.

Stellin (1995-97b) argued the following:

> When you customize a page at a web site, information about your preferences is stored on your hard drive in your browser directory. The ability to personalize web pages relies on a technology called cookies that works with most browsers. (p.1)

Cookies and Java Script have been a major concern for individuals who use Netscape Navigator 2.0. and other major browsers. For instance, Staten (1996) stated, "Java scripts can be sent to a browser whenever a particular page is requested. These scripts can perform a range of tasks from scrolling text to launching an applet" (p.1). Java Script can also track and monitor an individual's visit on the Internet. Monitoring can be done by using Java script to recall an individual's real name and electronic mail address from the Netscape rache file.

Cookies, a new technical device used by Microsoft Corporation and The Netscape Navigator monitor one's actions on the web (Gomes, 1996). Privacy Rights Clearinghouse (1997) (cited in Privacy in Cyberspace) defined cookies as, "A feature of many web browsers defined as client-side persistent information. Cookies allow web sites to store information about your visit to that site on your hard drive then, when you return, cookies will read your hard drive to find out if you have been there before" (p.7). According to Gimon (1997), one can not have more than 300 cookie files on their hard drive. If a users receives 301, the oldest one will be deleted. One particular web site or advertisement can not send more than 20 cookie files.

According to Netscape Communications Corporation, must cookie files have an expiration date on the file when it is deliver. However, if an expiration date is not provided, the cookie file is deleted once the user exits out of the browser. The major pitch the browsers have given about cookie files is that they have capabilities of storing personal

information about a certain site. To illustrate, once someone purchases something from a particular site, the cookie files are used as a resource base for the company. It provides general information to them without having to ask the patron to re-enter their personal data if they decide to return to that particular site. Nonetheless, the user would have to re-enter their personal information at a new site.

One major disadvantage about cookies according to Yang (cited in Staten, 1996) is, "A webmaster could pretend to be a particular site in order to retrieve a user's cookie data without authorization. If you use a server that does not encrypt its information, there is a real problem" (p.3). Cookie files can only be accessed by the site where the file was created; nevertheless, if a cookie file is placed on the hard drive it is possible anyone who has access to the site could view what is on the file. Web sites can only read cookie files that their particular web site has created, they can not read cookie files from another web site. According to Stellin (1995-97b), cookies are used for tracking purposes. Cookies allow the search engines to place a file on your hard drive. Once the cookie file is placed, the search engines have the ability to see where you are going while you are on the web. Gomes (1996) proclaimed, "Cookies are built into browsers and can not be turned off, while deleting the cookie file on your computer well erase any information, it will simply create a new cookie file" (p.2). The original intent of cookies were meant to be a benefit to the user. As Eichclberger (1997) proclaimed, " Cookies were intended to be a time saving device for computer users. Cookies were first develop so the information on the web could have longevity when viewed from one site to the next (Gomes). Netscape Navigator and Microsoft Network have insisted cookie files have a legitimate purpose; nevertheless, Netscape and Microsoft do agree that cookie files could cause major problems with an individual's right to privacy. Netscape has also stated they do not monitor the users every move, but they do occasionally view what the individual is doing while they are at a particular site. Cookie files will not inform another web site of your name; however, it can tell the web site that a particular computer has previously been to a certain web site.

Internet privacy advocates have stated there are several reasons why cookie files violate one's right to privacy. Cookie files can be connected to a larger database with or with out one's knowledge. For example, in some incidents cookie files are placed on the user's hard drive without the knowledge. Eichelberger (1997) stated, "Cookies were placed anonymously and without altering the user"(p.2). To illustrate, some cookie files are not clear as to who is the original sender of the cookie file. There have been some incidents were individuals have received a cookie file and did not know if the file came from the web site or the banner advertisement on the web page.

In addition to putting cookie files on to your hard drive, commercial on-line services are capable of saving copies of your messages. In some cases commercial on-line services such as Netscape Navigator, America On-line, CompuServe and Microsoft Network have provided copies of the messages to law enforcement agencies.

Chat Rooms give the misimpression they are private but this is not the case. On several occasions, the service provider will state the chat room activities are private. Nevertheless, the users of the chat room are able to store, capture, and transmit the conversation to individuals outside of the chat room (Privacy Rights Clearinghouse, 1997).

Browsing patterns, also known as transaction-generated information, is other way the users of the World Wide Web actions are monitored. For example, transaction generated information is used to collect users on-line interest. Privacy Rights Clearing House (1997), "The practice of collecting browsing patterns is increasing, on-line users should be aware that this practice poses a significant threat to on-line privacy" (pg. 4).

Matchcodes are another new technical system that violates a person's right to privacy on the web. Roger (1997) pointed out, "Matchcodes are unique identifiers used to pick information about consumers out of databases, much as banks use social security numbers to identify customers" (p.1). Matchcodes are used to track the users where abouts and then compare the places the user has been with information the system has on their

database. This is done to determine if the user would be interested in purchasing something off of the database. Roger discussed the following:

> Yet at the same time, the system has the ability to track the movement of any Internet user across participating sites, potentially revealing a dizzying array of confidential information, including users' reading habits, health concerns, political inclinations, and religious affiliations. (p.3)

Monitoring: Office Environment

Privacy issues are increasing between the employer and the employee. For instance, employers randomly observe a workers' electronic activities: Internet use, electronic mail, or voice mail, has been thought of as a invasion of privacy (Redell, 1992). Employers have the legal right to read employee's electronic mail without informing them of their actions. According to Kelly (1996), while mail sent through the postal service is protected by privacy laws, corporate electronic mail is not. Courts have not protected the privacy rights of those whose electronic mail messages have been read by their companies. The law does not provide or guarantee employee's privacy rights when using electronic mail at work. Privacy issues concerning electronic mail have caused the United States Supreme Court to interpret the Fourth Amendment's guarantee of privacy in novel ways. The Fourth Amendment protects individuals from government intrusion into their privacy ; however, this does not apply to private employers. The court has ruled citizens have the right of privacy from invasion of their phone calls or mail, but not electronic mail. Legally, electronic mail communications should have the same privacy protection as telephone calls. As Posch (1996) reported, "Electronic mail is equivalent to sending a postcard, nevertheless, electronic mail does not have the same constitutional free speech and privacy processions offered to telephone calls and first class letters" (p.2). Employers have the right to monitor their workers electronic mail, voice mail, and computer transaction without providing notice to the employee. Employees have no right to their personnel privacy while on the company electronic mail system. For example, employees have been

terminated after their employer monitored their electronic mail transmissions. When employees tried to challenge the termination, most court system have not agree that the employees privacy rights have not been violated (Bianchi, 1996). According to Bianchi, the decision to terminate an employee because the employer decided to monitor the employees' electronic mail is unfair to the employee. Companies may monitor; however, very few have guidelines or policies dealing with employees use of electronic mail and the Internet. There are limited rules and regulations on a written company policy that can help the employees understand the way employers monitor their use of electronic mail. Individuals using electronic mail and other cyberspace activities at work, believe the law will protect them when using an electronic mail account at the office, no matter if the electronic mail message is work related or not. Unfortunately, the laws that do exist do not protect the workers when they are being monitored at the office. As Besson (1996) acknowledged, "While the "Omnibus Crime Control and Safe Streets Acts of 1968 prohibits employers from eavesdropping on the private phone conversations of their employers at work, there is no similar protection of electronic mail communications" (p.5). In 1995, a survey was conducted by MacWorld (cited in Arbuss, 1995). The findings of this survey suggested that 30% of the companies that were surveyed, at least 1000 employers or more occasionally view their worker's activities. At least 25% of the employers stated that they viewed their employees computer files more than they read their electronic mail transactions. Nevertheless, more employers monitored their employee's electronic mail transactions when compared to monitoring the employee's voice mail activities. According to another survey conducted in December of 1995 by the Society for Human Resource Management (cited in Stellin, 1995-97a), 36% of the companies with electronic mail monitored their employee's transactions. These companies stated the reason they monitor their employees are for business and security reasons. Seventy-five percent of the employees stated their employers should be allowed to monitor their electronic mail.

In addition to monitoring electronic mail usage, supervisors also track their worker's Internet activities and watch how long they are on the phone. Another study was conducted by Network World Magazine of April 1997 (cited in Stellin, 1995-97a). The findings stated 70% of employers that were surveyed felt their employees use the technology that was available in their offices for purposes other than work, which meant that extracurricular activities where being done on company time.

Certain software programs allow employers to monitor what employers are doing on-line, including the web sites they viewed and how long they where there. Some other programs allow employers to deny access to certain on-line activities or place limitations on the amount of time the employees have access to certain electronic activities. Some of these software programs also have capabilities of determining how many pages were printed, where did they go while on line, what files where being copied and what was said on the employee's electronic transaction without the person's knowledge (Stellin, 1995-97a). Stellin (1995-97a) discussed the following:

> Sophisticated search capabilities make it easy to glean certain keywords like sex or resume. Even if your network doesn't automatically keep copies of electronic mail, its probably programmed to make backups. When you read your electronic mail a copy is downloaded to your hard drive, so when the network gets backed up, your mail gets copied, too. (p.6)

Employers also insisted security was another primary concern with the electronic transaction. Employers believe electronic mail provided employees possibilities to furnish important information to someone outside the company. Other reasons employers insisted they monitor their employee's electronic mail, is to prevent themselves from a future law suit for harassment, racism, sexism, or scandals (Stellin, 1995-97a). As of 1986, The Electronic Communications Privacy Act (ECPA) is the only federal legislation that deals with electronic snooping. Stellin (1995-97a) proclaimed, "The problem: ECPA specifically provides an exception for the provider of the service, which the courts have interpreted as

including employers"(p.3). In 1993 Congress proposed The Privacy for Consumers and Workers Act. This bill proposed that companies would be required to notify the employee. However, after being referred to the committee on Labor and Human Resources it was never considered any further (Stellin, 1995-97a).

Monitoring: School Environment

When compared with the office environment, universities are better prepared in dealing with policy agreements associated with electronic mail use and privacy rights. However, universities have legal rights to monitor students' and teachers' activities while using the web. Unfortunately, numerous assumptions are applied to the uses of the Internet in the school environment. Individuals at universities do not realize electronic mail activities are not private and every time a student logs on to a computer, information is collected about them without their notice (Descy, 1997). Several teachers and students at various universities believe electronic mail has the same legal protection as snail mail, this is not the case. As Descy pointed out, "Teachers and students should be aware that e-mail was not, is not, and will never be the sole property of the sender or the receiver" (p.49). To illustrate, a school is considered a public agency.

In several states, any electronic mail message that comes from a public agency is thought of as public information. According to Descy, if a message is going through a computer system and the operator of that system reads the message, the system operator is not breaking the law. It is critical that students and teachers that frequently use the institution's electronic mail system are aware when they delete messages that does not mean that the message is gone (Descy). As Descy stated, "The directory name may disappear, but the actual transmissions may not" (pg. 49). To illustrate, individuals in government agencies have stated they think it is necessary for the actual disk where the transmission is located to be overwritten a minimum of three times in order to feel secure the information will not re-appear.

However, it is still conceivable that even if a disk is overwritten numerous times the actual message may still be readable. Most institution's computer systems have capabilities of making back ups of one's electronic mail activities. The institution keeps the information that is backed up for months, sometimes years. There have been incidents were criminal activities have taken place and once the school suspects a certain individual, the school would look up the so called "delete" files to determine if there is any evidence of wrong doing (Descy, 1997). Teachers and students should be greatly cautious on what is said on the institution's electronic mail system. According to Stellin, at most universities a student's electronic mail account is regarded as private, unless some type of legal issue occurs. However, the government has to have school permission to read a student's electronic mail account.

The Internet has the capabilities of determining who you are and what you are doing. This is accomplished two different ways, voluntarily or involuntarily. It is not uncommon for teachers and students to complete forms such as catalogs, contests, or newsletters while browsing the Internet. Descy (1997) reported, "Every time a user fills out a form or inputs any data into a web browser, that information is transmitted to the host computer" (pg. 49). When teachers and students complete forms on the Internet, the user is voluntarily saying you may keep my personal information, unless the forms states otherwise. Involuntarily providing information happens every time an individual sends an electronic mail, or logs on to the web. Descy (1997) stated the following:

> Each login is broken down into statistics for file accessed, traffic by date, hour of the day, day of the week, domain of origin, and client reversed subdomain, and it keeps a list of all of the address of the accessing computers along with times accessed and number of files, bytes, and packets sent. (pg. 50)

Webstat, a simple application, has the capabilities of collecting information from commercial and educational computers as well as collecting information from computers from other places in the world such as Japan, Australia, Sweden, and Switzerland.

According to Descy, once the information is collected, it is cross-tabulated and placed in a file for future purposes.

Encryption: Privacy Protection

Privacy protection can be accomplished through several different means. Cryptographic technology is a significant concept being widely used for security protection. Encryption technology and digital signatures are two essential functions of cryptographic technology (Electronic Commerce ,1997). Electronic Commerce and European Union (1997) proclaimed, "Digital signatures can help to prove the origin of data authentication and verify whether data has been altered"(p.1). Government officials are not concerned about digital signatures being a problem, because one can still read the information. The Electronic Commerce and European Union insisted, "Digital signatures could even bring significant law enforcement benefits as they allow for example messages to be attributed to a particular reader and/or sender" (pg. 2). "Encryption can help keep data and communication confidential" (pg. 1). Many privacy advocates feel the best way to accomplish confidentiality in cyberspace activities is encryption technology (Arbuss, 1995). Encryption technology devices are inexpensive and an exceptional way to protect one's cyberspace activities (Redell, 1992). With encryption technology, it is possible to send or store information and not have to worry about other individuals reading the message. Privacy Rights Clearinghouse (1997) insisted, "The privacy advantage of encryption is that anything encrypted is virtually inaccessible to anyone other than the designated recipient"(p.6). Prior to the late 1970's The National Security Agency (NSA) had complete control of encryption technology in the United States.

Encryption technology has recently been a major issue between the government and the public sector (Ali, Hecker, Hoffman, and Huybrechts, 1993). The Federal government is distressed about the possible advancement of encryption technology. For example, a Federal grand jury spent three years investigating a popular encryption program, Pretty Good Privacy. Zimmerman (cited in Stellin, 1995-97a) founder of Pretty

Good Privacy disputed, "We live in a world that requires digital information to be moved around by everyone. This means that everyone needs cryptography. It isn't just for governments anymore" (p.6). The Federal Government is apprehensive that criminals and terrorists will manipulate this new technology. Recent studies have found encryption has played a major role in several criminal activities. Individuals conducting the study believed that as encryption technology advances so will criminal activities. The Federal agencies, including: The Federal Bureau of Investigation (FBI), The National Security Agency (NSA), The Central Intelligence Agency (CIA), The Department of State, and The Department of Justice, feel it is imperative that guidelines are established before encryption technology becomes a house hold utensil (Ali, Hecker, Hoffman, and Huybrechts, 1993). However, individuals in society have suggested powerful laws about encryption technology would violate their privacy rights. Corcoran (1997) stated, "Encryption is becoming a big business because in a world where information is as valuable as gold, people want to have some way to lock it up" (p.2). Wiretapping is one of The Federal Bureau of Investigation's (FBI) primary concern about the wide spread use of encryption technology. Previously, the FBI has collected a huge portion of their evidence through wiretapping. Nonetheless, several developments in technology have made wire tapping much more difficult than it has been in the past. Prior to fiber optics, copper wires were used in telephone lines, this allowed wiretapping considerably easier for The FBI. The wide spread application of encryption technology in the private sector, would cause the FBI to have an even more difficult time collecting information from wiretapping.

Two bills were presented on Capitol Hill in the summer of 1997 concerning privacy and technology. Corcoran (1997) stated, "The issue: How tightly should the government regulate the digital means of protecting information, known as encryption technology?" (p.1). The Senate wants to incorporate a plan allowing law enforcement agencies, such as the FBI, CIA, and NSA access to encryption technology to get information when needed. Freeh (cited in Corcoran, 1997) director of the Federal Bureau of Investigation stated, "If

encryption technology without spare keys is widely used, it will ultimately devastate our ability to fight crime and prevent terrorism" (p.3). According to Corcoran, if the Senate bill is approval it could be very costly for everyone involved, not to mention the lack of privacy protection for individuals that use encryption technology. The primary reason the government has insisted on having access to an individuals encryption technology is to intercept any criminal activity.

For several years the Clinton Administration has been trying to organize a plan that would satisfy the general public and the private sector, in addition to allowing the government legal access to view electronic transactions (Corcoran, 1997). Having access to everyone's encryption technology would allow the government to have a system similar to having a spare key to a person's car or house. The spare key system, or the back door approach, would be placed at a central location. If the key access center is enforced, critics argued, (Corcoran) "Encryption technology would only be used by the so called good guys. Criminals would still find a way to use encryption technology for criminal acts" (p.2). Advocates of privacy organizations believe the government having access to a person's encryption technology is questionable.

Privacy Laws

An Internet users privacy rights are limited when it deals with protecting your personal information. As Stellin (1995-97b) stated, "You have even fewer rights in the uncharted and un-legislated territory of the Internet. The development of privacy law concerning information gathered off line has been so haphazard that the outlook is glum for information gathered on-line" (p.1). According to Descy (1997), very few people are not aware that the Internet has it own set of guidelines and is not governed by the usual rules and regulations. The only government organization addressing the privacy issue in the electronic age is The Information Infrastructure Task Force. The Information Infrastructure Task Force has released a proposed privacy guideline to help regulate personal information gathered on-line (Stellin, 1995-97b). Nonetheless, these guidelines are only touching the

surface of the privacy issues dealing with cyberspace. Stellin (1995-97b) proclaimed the following:

> Essentially, these privacy principles are intended to govern how information is acquired, used and disclosed on the net by requiring that business inform consumers why they are gathering data, what it will be used for, what steps will be taken to protect it, and how consumers can correct any in accuracy. (p.21)

Government legislation is needed in order to protect the general public concerns with privacy. Besson (1996) stated, "Legislators have been slow to react to the information age. Courts are struggling to apply old privacy concepts to the new medium of cyberspace, and have not yet resolved many ambiguities in new electronic privacy laws" (pg. 1). Compared with other countries, The United States current privacy protections are deficient. The United States is trailing other country's policies on protecting consumer's personal information. For example, The European Union is in the process of implementing a legal protection program requiring the private sector to have and enforce certain security measures when dealing with technology. These guidelines protect a user's personal information when collected by unauthorized individuals (Stellin, 1995-97b). According to Stellin, having guidelines on electronic mail and another cyberspace activities would help. Nonetheless, it will not replace the issue of guidelines and laws needed to be addressed by Federal Legislation.

Several of the laws and regulations established for protecting one's right to privacy were developed during a period when technology was not so advanced (Besson, 1996). According to Givens (1997), the privacy laws dealing with technology in the US are inadequate and have not kept up with the rapid growth of technology. Givens stated, "The US has addressed it sector by sector, industry by industry. The result is a patchwork of laws with significant gap" (p.2). Many individuals believe the Fourth Amendment protects them when they are interacting on the web; however, this is not the case. As Arbuss (1995) reported, "The Fourth Amendment of the United States Constitution protects

individual's privacy from government intrusion. The Fourth Amendment does not apply to acts of private companies or individuals" (p.2). The First, Fourth, and Fifth amendment all deal with one or another aspect of privacy protection but none of them deals with protecting an individual's right on-line. California is an exception to this rule because they have established their own rights to privacy under the California constitution. But, the California constitution does not apply to situations that deal with the government.

The Privacy Act of 1974 does not cover ones personal information collected on the Internet. Givens (1997) proclaimed, "The Privacy Act of 1974 covers citizens' relationships with federal government agencies, and doesn't touch on the private sector at all" (p.3). The rules and regulations on privacy rights in cyberspace differ depending on the individual who is conducting the monitoring. According to Besson (1996), employers, the government, the Internet, Service Provider, and third parties all have different rights when it deals with monitoring cyberspace activity. For instance, the Electronic Communications Privacy Act has different penalties for electronic mail messages. The penalties vary depending if the message is in transmission or if the message is stored. Besson defined, "Stored messages, may include messages in the addressee's mailbox waiting to be picked up by the addressee, and records of private on-line discussions between users"(p.4). Title one of the ECPA penalizes the government, service provider, and a third party from intercepting a message. Title two of ECPA penalizes the third party and the government. Legally, the system operator can view a person electronic mail message under the exceptions of the ECPA. Large commercial service providers, including CompuServe or America On-line or local Internet service providers all have on-line service agreements. The Service providers agreement could limit the individual's privacy rights granted under the ECPA. Besson proclaimed, "Unfortunately, most users do not realize they are signing away privacy rights when they go on-line through a service provider, because most service agreements are "take-it-or-leave-it" contracts" (p.6). Nonetheless, the ECPA has established some guidelines that will help the individual with local and

commercial service providers. For example, Title I of the ECPA, does not allow the operator of the system to hinder a electronic mail or chat room messages during transmission. Title II of the ECPA gives the operator of the system permission to review what is a stored message, but it prohibits them from revealing the contents of the message to a third party individual including the government. Individuals who feel as if their privacy has been violated by the Internet service provider can look to the ECPA guidelines to determine if any part of the law will apply to their particular situation. Under the ECPA, the Internet service provider can not provide an user's personal information to the authorities without proper documentation, such as a subpoena. The Omnibus Crime Control and Safe Streets Act (1968) (cited in Posch, 1996), dealt with threats to privacy resulting from the growing use of electronic monitoring devices that threatened an average citizen's privacy. The Omnibus Crime Control and Safe Streets Act (1968) pertained to only wire and oral communications. The 1986 Electronic Communications Privacy Act (ECPA) was originally passed to prevent telephone wiretapping. The ECPA was revised in 1986 to include all forms of digital communications, which also covers electronic mail activities (Besson, 1996). Privacy Rights Clearinghouse (1995-97) illustrated, "The Federal Electronic Communications Privacy Act (ECPA) makes it unlawful for anyone to read or disclose the content of an electronic communications (18 U.S.C. 2511). The law does apply to electronic mail messages" (p.3). Nonetheless, there are limitations to the act. The Privacy Protection Act (PPA) was passed by congress in 1980. Besson stated, "The PPA prohibits law enforcement from searching or seizing "work-product" and documentary materials from journalists and publishers unless they have "probable cause" to believe the person possessing the materials is involved in the crime, and the materials sought are evidence of the crime" (p.4). According to Besson, under the PPA, the actual system and the individuals who patron the system are protected by the PPA as long as the person is acting as a publisher of some kind or maintains published property. Maintaining

published property on the web would include web pages, electronic mail, newsletter, and databases not readily available through any other means but the Internet.

CHAPTER THREE

Summary

Alder defined (cited in The Internet and privacy: Do you know who's watching?, 1996), "Privacy Issues in Telecommunications as: the right not to be disturbed, the right to be anonymous, the right not to be monitored and the right not to have one's identifying information exploited" (p.1). Individuals that use various telecommunications are being disturbed, monitored, and violated in numerous ways. This review of the literature of has demonstrated that the rapid growth of technology has definitely increased the privacy issues with one's right to privacy in the government arena, private sector, higher institutions of learning, and the general public. There is no question that there is a need for some sort of "adequate" guidelines and regulations to exist which can assure the user that various telecommunication activities are private.

The question now becomes will inadequate privacy laws dealing with cyberspace have an effect on future technological applications and activities? Will privacy issues cause individuals to be afraid of telecommunications? The advantages of technology are definitely larger than the disadvantages of the privacy issues dealing with technology. Nonetheless, the issue of privacy and cyberspace has many users concerned. As addressed throughout this paper, the issues are as wide spread as the technology it self. As Besson (1997) reported, "There remains much to be done to secure the fundamental right of privacy in the new sphere of cyberspace" (pg. 10). In providing a solution for privacy protection in cyberspace, it is not clear if better technology is necessary, more comprehensive privacy laws, or a combination of the two. However, what is clear is that everyone involved with technology including the designer, builder, operators, and maintainers, realize the responsibility of privacy protection. Privacy and cyberspace can not be left alone for the Federal government to handle. It is important for all members of the technology community to become stakeholders in the future of privacy protection in cyberspace. The government, commercial enterprises, educational institutions, and non-

profit organizations all have been involved in the growth of cyberspace and should be involved in the growth of proper laws and guidelines dealing with privacy protection and cyberspace. Technology will continue to expand at a rapid pace, and it is up to everyone involved to make a valid effort in order to ensure the laws and regulations dealing with privacy in cyberspace expand as well.

REFERENCES

Ali, A. F., Heckler, L. S., Hoffman, J. L., and Huybrechts, A. (1993). Cryptography:Policy and technology trends. [On-line]. Available: http://www.vortex.com/privacy/crypt~plcy.1

Arbuss, S. (1995). You own your web. [On-line]. Avaliable:http://www.paranoia.com/~ebola/yow.html

Besson, A. (1996). American Civil Liberties Union:Cyber-Liberties. [On-line]. Avaliable:http://www.aclu.org/issues/cyber/priv/privpap.html

Bianchi, A. (1996). E-mail privacy: Fact or fallacy? Inc.18, 100.

Cheshire Network. (1997) What is an applet? [On-line]. Avaliable:http://www.cheshire.net/faq/applet.html

Corcoran, E. (1997) Who will hold the key? Two Bills Reflect the Split Over Restrictions. Washingtonpost.com. [On-line]. Available: http://www.washingtonpsot.com/wp~sev/tech/analysis/encryption/issues.htm#Top

Descy, D. E. (1997) The Internet and education: Some lessons on privacy and pitfalls. Educational Technology 37, 48-52.

Electronic Commerce and the European Union. (1997) .[On-line]. Avaliable:http://www.ispo.cec.be/eit/policy/97503.html

Eichelberger, L. (1997). The cookie controversy. [On-line]. Available: http://uts.cc.utexas.edu/~ccfr362/index.htm

Epic On-line Guide to 105th Congress Privacy and Cyber-Liberties Bills. (1997). Electronic Privacy Information Center. [On-line]. Available: http://www.epic.org/privacy/bill_track.html

Gattiker, et, (1996) The Internet and privacy: Do you know who's watching?., Business Quartely 60, 79.

Gimon, A. C. (1997). How the cookie crumbles. InfoNation Magazine. [On-line]. Available:http://www.info-nation.com/cookie.html

Givens, B. (1997). Privacy Rights Clearinghouse. [On-line]. Available:http://www.privacyrights.org/ar/jtta.skap.html

Gomes, J. (1996). Web 'cookies' may be spying on you. Mercury Center/San JoseMercury News. [On-line]. Available:http://cgi.sjmercury.com/business/cooki212.htm

Kelly, K. (1996). Cover story: A e-mail problem. Wall Street Journal Report.

Miller, L. (1997) On the Internet, virtually no privacy. USA Today Tech Report. [On-line]. Available:http://www.usatoday.co/life/cyber/tech/ct019.htm

Information Security and Privacy In Network Environments. (1994). [On-line]. Avaliable:http://cpsr.org/cpsr/privacy/crypto/ota_report_1994/8pager.txt

Netscape Communications Corporation. (1997). Cookies and privacy FAQ. [On-line]. Avaliable:http://search.netscape.com/assist /security/fags/cookies.htm#are_different

Network Solutions. (1996). What is a search engine? [On-line]. Avaliable:http://199.76.196.134/pages/web6_search_engines/sld02.html

Ongoing Java Script Development. (1997). [On-line]. Avaliable:http://www.geocities.com/SiliconValley/Park/3091/introd.htm

Plymouth State College. (1997). What is a Web Browser? [On-line]. Avaliable:http://www.plymouth.edu/infotech/webbrowsers.htm

Privacy In Cyberspace:Rules of the road for the Information Superhighway. (1995-97). Privacy Rights Clearinghouse. [On-line]. Available:http//www.privacyrights.org/fs/fs18-cyb.html

Posch, R. (1996). E-mail and voice mail: Basic legal issues for corporate. Direct Marketing, 58, 54.

Redell, D. (1992). Information technology and the privacy of the individual. [On-line]. Available:http://www.vortex.com/privacy/acm-wpd.1

Rodger, W. (1997). Ad tracking technology sparks new privacy war. Inter@ctiveweek. [On-line] Available: http://www.2dnet.com/intweek/daily/970919f.html

Rotenberg, M. (1992). Proposed privacy guidelines for the NREN [On-line]. Available:http//www.vortex.com/privacy/cpsr-nren.

Staten, J. (1996). Netscape tricks raise security concerns. MacWeek Gateways. [On-line]. Available:http://www8. 2dnet.com/macweek/mw_1011/gw_net_tricks.html

Stellin, S. (1995-97a) Privacy in the digital age: Part 1: Who's watching you on-line? [On-line]. Available:http://www.cnet.com/content/Features/Dlife/Privacy/

Stellin, S. (1995-97b) Privacy in the digital age: Part 2: How private is your personal information? [On-line]. Available:http://www.cnet.com/content/Features/Dlife/Privacy2/

What Is a Chat Room? (1997) Netscape Communications. [On-line]. Available:http://home.netscape.com/eng/chat/2.0/handbook000000009.htm