1-1-2002

WwwPrivacygov: A constitutional and legislative review

Stephanie Ann Murphy
University of Nevada, Las Vegas

WWW.PRIVACY.GOV: A CONSTITUTIONAL AND LEGISLATIVE REVIEW

by

Stephanie Ann Murphy

Bachelor of Arts
University of Nevada, Las Vegas
1997

A thesis submitted in partial fulfillment
of the requirements for the

Master of Arts Degree
Department of Political Science
College of Liberal Arts

Graduate College
University of Nevada, Las Vegas
May 2002

UMI Number: 1411199

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

UNLV

Thesis Approval
The Graduate College
University of Nevada, Las Vegas

April 17, 2002

The Thesis prepared by

Stephanie Ann Murphy

Entitled

WWW.Privacy.Gov: A Constitutional and Legislative Review

is approved in partial fulfillment of the requirements for the degree of

Master of Arts in Political Science

Examination Committee Chair

Dean of the Graduate College

Examination Committee Member

Examination Committee Member

Graduate College Faculty Representative

PR 1017-53 1-00

ABSTRACT

WWW.Privacy.gov: A Constitutional and Legislative Review

by

Stephanie Ann Murphy

Dr. Michael Bowers, Examination Committee Chair
Professor of Political Science
University of Nevada, Las Vegas

One of the most controversial and evolving rights recognized within recent years has been the right to privacy. During the twentieth century, the Supreme Court and the United States Congress recognized the existence of this right, although in limited aspects. In the twenty-first century, Americans' privacy rights have clashed with the evolution and the use of the Internet. Complications between a person's privacy and the information needed for national security interests arose. The following study examines the question of where the privacy of an individual in this new era ends and where government intrusion begins. Through a qualitative analysis, constitutional and legislative aspects will be brought forth to challenge the idea that self-regulation is feasible within the growing cyber nation. Final analysis will bring forward new policy proposals to counter current problems in this virtual world.

ACKNOWLEDGMENTS

I would like to thank my family, who have been so supportive and understanding throughout my scholastic career. Without their love and sense of humor, I would not have been able to finish with my sanity still intact.

I would also like to extend my gratitude and appreciation to Dr. Michael Bowers, for being so patient with me and my endless questions; Dr. Ted Jelen, for encouraging me to pursue my masters as well as becoming a committee member at the last minute; Dr. Alan Zundel and Marianne Zundel, for their support and enthusiasm; and Dr. Gary Larson, for also becoming a committee member on short notice.

Lastly, I would like to thank Melanie Young, Cathlena Boyd, Erin Buck, and Brian Rassmussen for allowing me to utilize their grammar skills and bounce off concepts. It has been a privilege and a pleasure to work with all of you. Do not forget to aim high and never settle in life.

INTRODUCTION

THE INTERNET

Since the 11th of September 2001, accusations of government law enforcement and intelligence agencies spying on citizens as well as observations about legislators' and the constituents' lack of involvement in current policy outcomes have become major issues to many users of the Internet, who refer to themselves as "Netizens." The right to privacy in this information era has become one of the most controversial issues today. Yet in the wake of the terrorist attacks on America, this unstable right has become more precarious than ever before. Questions of where the government can intrude have been raised. However, with legislation such as the USA PATRIOT ACT and programs such as DCS1000, one must ask whether there is a protected constitutional right to privacy, and if so, who or what will protect that right?

This thesis examines the problems that American Netizens face on the Internet in the aspect of privacy. Chapter One addresses the history of the Internet as well as the growing problems of government encroachment on citizens' privacy rights. Chapter Two discusses the Supreme Court's rulings on whether or not government has the ability to impose electronic surveillance on the citizens' constitutional right to privacy from government intrusion. The third chapter reveals Congress's decisions on the growing privacy problems in respect to new technology. In addition, it will also address the USA PATRIOT ACT. The final chapter is a summary of the preceding chapters and answers

the question of whether or not the government believes that American Netizens have a right to privacy on the Internet. In addition, some proposals will be given to address the question of who will protect the Netizens' rights.

CHAPTER I

WELCOME TO THE JUNGLE

The Internet is a mysterious word that conjures up ideas of digital or laser wires interlinking and overlapping one another, spanning across the ether of virtual space to link human interactions between numerous people. Fantasy images of this network, created by mad scientists, are epitomized in movies such as "Tron," "Hackers," and "The Net" which create an environment that pits the good against the bad hackers.[1] The idea of the Internet has become romanticized in today's world. Yet very few people who interact and use the Internet know what its capabilities are, and what the dangers are that hide beneath its surface. Most people, until recently, believed the Internet was a safe haven for many who wished to enter a new unknown world. However, with modern technology, this is all changing, and the users' privacy becomes more of an issue than ever before.

While the word Internet (National Information Infrastructure- NII) seems innocent, there are many untold dangers that await those who have yet to travel the wrong cyber

---

[1] "Hacker" is a term that denotes a person who attempts to gain unauthorized access to a system, but does not seek to do any damage. It also refers to computer users who experiment with computer programs to test their limits. A "cracker" is a term that has been proposed to refer to computer criminals, who unethically and illegally obtain access into systems. (Meyer and Baber 1997, 8-7)

road in this digital world.[2] Every day, millions of people around the world turn on their computers and log onto an Internet Service Provider (ISP), which will allow them to access the World Wide Web (web). People access their bank accounts, talk to or e-mail their friends and family, go shopping, plan trips, watch movies, listen to music, and read the news through the NII. Some people access information on their representatives and pending legislation, sending electronic mail messages (e-mail) to state and federal representatives. In some states, one can even cast his or her ballot in elections instead of taking the trip down to the polls. Nowadays people even work at home, submitting their work through e-mail to their companies, or they run small businesses using a web site. While the advantages of the Internet are seen on a daily level, there still are many dangers or possible dangers that users face when interacting with others.

As one can see from the previous list of Internet interactions, one of the chief dangers in this new society is that of releasing too much information about one's self allowing one's privacy to erode, even if indirectly. People argue that companies are becoming too inquisitive, asking too many personal questions, or giving out too much information about individuals. Yet people are still willing to submit their information to an unknown other, without asking questions. People seem to forget about him or herself as an individual and his or her protected rights. Moreover, there are still many who have forgotten that people are not the only factor involved in today's world, computers also play a huge role as well as the government and its interactions. Perhaps, by taking a look at the government and its relationship to the Internet, as well as how the Internet has

---

[2] Some analysts of the Internet refer to the Internet as the National Information Infrastructure (NII), and the proposed Information Superhighway as the Global

evolved, one can see the attempts made to erode the individual's newfound privacy right.[3]

The Birth of a New World

The history of privacy on the Internet is a rather short one when compared to traditional rights such as the right to protect one's property or the freedom to practice one's religion. In 1969, the Advanced Research Projects Agency (ARPA) was contracted to connect four university computer labs: UCLA, Stanford, UCSB, and the University of Utah. The experiment was to provide a "communications network that would work even if some of the sites were destroyed by nuclear attack. If the most direct route was not available, routers would direct traffic around the network via alternative routes." (Howe 1998, 3) The network was also to facilitate cooperation between several research sites and eventually the military, as well as ensure the physical security of the data and information available on the system. (Barrett 1996, 21) The experiment proved a success; so between the end of December 1969 and by June of 1970, four additional institutions decided to become a part of the network. (Howe 1998, 3)

The 1970s brought additional institutions online. The ARPA-established network had been dubbed ARPANET, and NASA, a military space program, had joined the ranks of institutions involved in this growing computer infrastructure. (Barrett 1996, 22; Howe 1998, 3) At this time, commercial interests in ARPANET did not exist. ARPANET was

---

Information Infrastructure (GII). I shall be using these terms interchangeably throughout the text.

[3] Chapter Two discusses the birth and history of this right.

dedicated to pure research and information, and monitored through the government agency ARPA. By the mid 1970s the basic foundations for the Internet had been established, but due to the complex computer languages involved, it was very difficult to access. In 1979, Usenet, a private institution, created a newsgroup system that was based upon a 1978 Unix to Unix Copy Protocol. Essentially, the newsgroup system allowed different users from different sites to access topic specific discussion groups. The significant aspect was that it established early community building on a network, even though at the time it was still not a part of the Internet due to differing programming architecture. These network communities would create the base foundations for the community of Internet users who would call themselves Netizens. (Howe 1998, 3)

By 1980, the network had grown unbelievably large, and so a portion called MILNET broke off.[4] The United States Defense Department adopted this communication network, but stipulated that there needed to be a way to connect both military and research networks in the future. The Defense Research Projects Agency (DARPA) undertook the task of connecting both networks to create DARPA Internet or DARPANET. DARPANET would eventually be referred to as the Internet. (Barrett 1996, 22)

At the same time DARPA was linking research and military networks, private corporations began to start their own networks. One of the first created was termed BITNET, referring to "Because its [sic] Time Network." (Howe 1998, 4) BITNET was connected to the IBM mainframes in the educational community around the world to provide mail services, as well as discussion groups similar to those designed by Usenet.

[4] MILNET is the military communications network.

In 1983, the DARPA Internet was universally accepted and adopted on a national level. By then, commands became easier for the normal person to access and learn. This opened up the Internet to multi-department usage in universities. Prior to 1983, departments in computer science and physics were some of the few departments that had the technological know-how to access the information. By the mid-1980s gateways had been developed to connect BITNET with the Internet. This provided not only the exchange of e-mail, but also linked the discussion groups so educational facilities could communicate in real time as well. (Howe 1998, 3-4) Unfortunately, with the increase in university additions the Internet sites started to become unmanageable.

The late 1980s and early 1990s saw the National Science Foundation (NSF) assuming DARPA's governing role. With the responsibility of governing the Internet also came an additional duty to create a gateway for the United Kingdom's Joint Academic Network (JANET)[5] to the Internet. At this time, the first attempts were made to index the Internet.[6] In addition, one of the prime groundbreaking inventions on the Internet was created. Tim Berners-Lee at the European Laboratory for Particle Physics (CERN) made the Internet easier to use by creating hypertext. (Howe 1998, 5) Hypertext allows a user to access another remote site by clicking on a specific underlined or highlighted topic-linked word. (Meyer and Baber 1997, 5-7) This invention would eventually link various chat sites as well as additional informational sites to a specific topic discussed on one

[5] Similar to ARPANET, this educational network linked the UK's finest universities.
[6] The first archiver of the Internet was Peter Deutsch from McGill University in Montreal. He created a program that would read the FTP (file transfer protocol) sites, and named this program Archie. Eventually other archivers, such as Jughead and Veronica would be created after Archie was terminated. (Howe 1998, 4-5)

web page, thus allowing users to easily and quickly access interest-related materials and discussions.

In July 1992, the first national commercial Internet Service Provider (ISP), Delphi, was permitted to open its electronic mail system to the public. Four months later all government imposed commercial limitations on Internet use had disappeared, making the Internet available to a variety of commercial interests. (Howe 1998, 5-6; Barrett 1996, 23)

The year 1995 saw the end of government control of American institutions on the Internet as the NSF released its sponsorship of the NII to the privatized ISPs, such as the newly created America Online (AOL), Prodigy, and CompuServe. This private control allowed for individuals not in the academic community to access the Internet through personal computers (PCs) and dial-up modems. The ISP provided a service that allowed home PCs access to the provider's supercomputers, the hosts, which would then allow the user access to the Internet through wide area networks. This created facilities that would be available to anyone who wished to take part in the Internet experience. (Barrett 1996, 23) In addition, the government's lack of involvement facilitated the new Netizens' feelings of independence and unprecedented freedom.

The final and most crucial step in introducing the Internet to future Netizens was in the 1998 release of Windows 98. Incorporated within the system was a new Microsoft friendly browser. This allowed thousands of people easy access to the Internet, where they in turn found information on a variety of topics as well as a way to meet other users to whom they could relate. (Howe 1998, 5-6) As a result, Internet communities began to

grow, and with them came political awareness in establishing and defending the net communities' personal rights.

Through the Internet's history, one can see the growth of a new world. At one time, government had taken an active role in the Internet. However, realizing that the Internet had social and market potential in addition to the research and information aspect, the government allowed private corporations to take over and make the rules. Eventually, the government would find that minimal intervention in the Internet was more lucrative to the United States' market economy. However, the lack of intervention also facilitated the rise in computer crimes. As a result, after several years of minimal government intervention and the allowance of private regulation through the ISPs, the U.S. government decided, as it did with other new technology throughout the 20th century, to use the Internet as a tool to capture criminals and deviants. The idea was to eliminate the then current private industry regulations created from the ISPs, since these case by case created regulations failed to hinder the increasing rise in electronic crime performed by crackers, regular enterprising criminals, and identity thieves. ("No Place to Hide," 2001) In addition, law enforcement agencies grew aware of the increasing use of electronic bombs, often referred to as e-bombs,[7] viral worms, and the discussions of an e-jihad.

[7] E-bombs can affect a system in a variety of ways. They are usually a computer virus attached to a file, which is sent through e-mail. The first experiences with e-bombs and viruses were seen around 1982. Since then they have evolved from immature programming glitches to intricate codes (macros) that have little programs within that reformat a computer's operating system and programs. (Buderi 1999, 34-36)

A Backdoor In

Since September 11, 2001 the government has come down even harder on Internet Service Providers (ISPs). Consequently, online privacy has taken a huge blow as legislators and law enforcement agencies weigh national security against the populace's privacy. The debate ranges from the continuance of ISP self-regulation to judicial and congressional sanctioned allowances of government intervention techniques. However, one of the most disturbing and disappointing aspects to result from the security debate after September 11th comes from the American citizens themselves. In a Newsweek poll taken during September 13th and 14th of 2001, "57 percent of Americans said that they would support eroding encryption protection to help law enforcement monitor terrorism suspects- even if it might affect privacy and business practices. Thirty-nine percent were opposed, the rest undecided." (Associated Press 2001, 2) This drop in concern for privacy would appear to support federal agencies, such as the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI), in initiating a variety of snoop programs. Perhaps in this new era of American vulnerability previous debates on encryption, DCS1000, keystroke logging, and anonymous proxies will fall to the side as a result of fears initiated through recent acts of violence, and the government will be able to intervene without restraints.[8]

One of the areas in which government wishes to take a stand is in the realm of cryptography, or encryption. Encryption, a highly debated issue, is considered one of the ultimate defenses against all those who are not supposed to access the information one person sends to another. In order to use encryption, one person must have the "key" to

---

[8] These terms will be discussed further in this chapter.

encrypt a message, and the other person must have a matching "decoder key" in order to read that message. Those who send sensitive or confidential information in communications and transactions, such as a credit card number or physical address, usually support encryption. In addition, encryption can be seen as a means of personal identification, like a signature, thus verifying that information sent from one party to another is legitimate. (Bennett and Grant 1999, 120) While terrorists and criminals can potentially use encryption, the current debate is whether or not encryption is less likely to be used by them since it would probably attract more attention to their communications, which is something they do not desire.

Nevertheless, the U.S. government is seeking access to American created encryption software, in hopes that by attaining an all access key, it can prevent criminal events. Unfortunately, the problem may not be so easily fixed because not all encryption software is created or made in the United States and the U.S. government cannot force foreign companies to abide by their demands for an all access key. Furthermore, even if the American companies provided the government with all access keys, why would a criminal knowingly use encryption software that law enforcement agencies had the ability to read? The more likely possibility is that American criminals would buy foreign encryption, even if it could be obtained only through the black market. These arguments are similar to the ones seen in the debate for and against anonymous proxies/posters and remailers. (Associated Press 2001, 2)

Anonymous proxies, posters, and remailers are services that allow people to access the Internet to engage in anonymous bulletin board postings and e-mail. There have been huge debates on the anonymity of remailers in the past few years. Originally they were

intended for psychological patients who were recovering from some traumatic experience or political dissidents who feared government retribution. But in recent years, hackers and crackers have adopted them as their sanctuary. In fact, many of the computer e-mail viruses released have originated from these remailers. (Buderi 1999, 36) While some remailers comply with governments' requests to release information on a user, most support the users' anonymity and consequently have been shut down through court injunctions and ISP sanctions for taking a stand to protect the anonymity and privacy of their members. (Anschütz 2001, 42-44; Levine 1996, 1526-1572)

One of the big winners resulting from the current fear climate will be Carnivore, recently renamed DCS1000.[9] Part of a covert FBI surveillance triad known as the "Dragon Ware Suite."[10] Carnivore is reportedly a stealthy looking black box outfitted with a Pentium III containing Windows NT, which is equipped with "packet sniffing software." (Cohen 2001, 50; Meeks 2001, 1). Essentially, when the FBI has identified a suspect whose e-mail they wish to peruse, they acquire a court order similar to a phone wiretap and take Carnivore out of storage from Quantico, Virginia. Then working in conjunction with the ISPs, who are under court order to comply and keep quiet about it, the program is installed into the network for the FBI. Once installed, Carnivore searches through e-mail traffic for a name, looking at "To" and "From" lines, IP addressees, and

---

[9] The renaming of Carnivore has to do with the negative implications of the name. While the program was named for "getting to the meat" of the information, the sinister name caused many complaints among online users. As a result, this FBI program was renamed to take away the creepy connotation. (Cohen 2001, 50)

[10] "Dragon Ware Suite is more than simply an e-mail snooping program: it's capable of reconstructing the web surfing trail of someone under investigation... [It can] reconstruct web pages exactly as a surveillance target saw them while surfing the Web...Besides Carnivore, the Dragon Ware Suite includes programs called 'Packeteer' and

keywords in the header or the body of the e-mail. According to the FBI, the software is "designed to spy with 'surgical' precision on specific individuals." (Cohen 2001, 50) (See APPENDIX III to find more information on Carnivore.)

For obvious reasons, critics[11] of Carnivore debate the merits of this program, stating that it endangers our society and our freedoms in allowing for the possibility of the Internet morphing into a massive surveillance system. Yet, the other side of the argument is that it allows law enforcement agencies to crack down on drug trafficking and other illegal activities. The pros and cons of the debate are strong on both sides; yet what critics usually forget is that the information the FBI can acquire truly depends on the kind of court order that the agency obtains. Court orders usually issued allow for the FBI to acquire e-mail addresses in a form that resemble those of a "pen-register" or a "tap-and-trace," which allow law enforcement agencies to get phone numbers off a telephone line.[12] However, in order for the FBI to gain the full substance of the e-mail, a full-blown content wiretap is required, which the courts are far less willing to provide. (Cohen 2001, 50)

Moreover, critics worry about the possibility of the FBI misusing its "tap-and traces" as well as "pen-registers." The government contends that these limited wiretaps entitle them only to the e-mail headers, yet some critics state that to obtain access to even the header, the FBI should have to meet the same high standards required for a content

---

'Coolminer.'... These data programs are used to reconstruct the raw data scooped up in the initial phase by Carnivore." (Meeks 2001, 2)

[11] The Following are some of the critics of the Carnivore program: civil libertarians; John Perry Barlow, co founder of the Electric Freedom Foundation; and Lee Tien, senior staff attorney with the Electronic Freedom Foundation.

[12] A "tap-and-trace" allows police to record the phone numbers a suspect dials. "Pen-registers" let the police log the phone numbers of incoming calls. (Cohen 2001, 50)

wiretap.[13] In addition, reviewers of the program debate whether or not Carnivore is as surgical as the FBI contends. The fear involves the likelihood of the FBI downloading information about non-targets that it may happen to intercept. The unspoken fear is that eventually the CIA and the FBI would be able to easily build a dossier on just about everyone. As a result, analysts would like to see legislation that requires the FBI to throw out collected evidence that is not involved in the investigation. Another possibility is that once the investigation is over, rather than storing the acquired information in a permanent database, purging that information would be obligatory. (Cohen 2001, 50)

However, with the current political climate seen in the United States and the media, advocates for privacy on the Internet are finding that they are fighting an uphill battle. In fact, the national mood may increase funding for other surveillance programs, such as the National Security Agency's (NSA) Echelon program, which is a global wire-tapping network. This system grew out of the 1945 joint agreement to share information obtained with the intelligence operations of New Zealand, Canada, and the United Kingdom. Very little is known about Echelon, but in a report given by the European Parliament in July 2001, not only was its existence confirmed, but also its ability to intercept any telephone conversation, Internet connection, e-mail, or worldwide fax. (Cohen 2001, 52) Like Carnivore, it can hone in on specific words, such as "hijack", "bomb", or "jihad" to name a few. However, it is debatable as to how effective Echelon actually is, since the system collects up to 3 million messages a minute, which then must be sorted through. Critics

[13] Headers are the headlines in the message box that summarize the contents of a message.

such as Adam Cohen contend that if this system were actually effective, September 11th would not have happened.

Echelon poses a real privacy problem in that it is a global system that intrudes without the required judicial oversight that even Carnivore must have. Moreover, Internet traffic travels in such a way that a majority of the world's e-mail and other communiqués cross over the United States' borders and then out once again. Not only is there concern about Echelon spying on foreign communications, but also those communications between Americans abroad and residents, who are supposed to be outside NSA jurisdiction. (Cohen 2001, 52)

Even without the use of DCS1000, encryption access, anonymous proxies' help, or Echelon, the increase of computer forensics in the law enforcement and intelligence fields will probably rise. One of the most interesting tools currently being used is that of keystroke logging. Keystroke logging essentially uses a suspect's computer keyboard against that person. Investigators secretly install hardware in the perpetrator's computer. The device then records each and every letter a person types into his or her computer, turning the computer into a mole for the agency.[14] Obviously this allows officials to view correspondence, at least from one end, as well as the prized passwords needed to unlock encrypted messages. (Dam and Lin 1996, 49) Furthermore, if one expands this unsanctioned activity, privacy, anonymity, freedom of speech, and the security of each

[14] Encryption and keystroke logging are often used in Information Warfare (IW). Other avenues used in IW include: physical destruction of facilities, degradation of the opponent's system through covertly using software and/or hardware, withdrawal of opponent's data, replacing it with misleading data, and using software as a mole against the opponent. (Dam and Lin 1996, 49

American are violated every time this technology is used for any reason, including the capturing and prosecuting of criminals.

In light of these government intrusions, questions revolving around a citizen's personal privacy arise. In Chapter Two, privacy is defined and outlined. In addition, government intrusion into a citizen's life, and how far that intrusion may go is also examined.

CHAPTER II

PRIVACY ALL GROWN UP

Privacy in the United States has become one of the most highly debated rights today. While there are many who claim that the right to privacy is a fanciful privilege, the proponents of that interest hold to the idea that it, like many other rights, is inalienable. Opponents of privacy rights, however, have a true advantage, in that the basis for this claim is said to be unstable. The major reason stems from the fact that, while the United States Supreme Court and the supporters of privacy rights derive this liberty out of the Constitution, there is no direct language in the document establishing the existence of privacy.

For many people, privacy is a difficult concept to define. Legal scholars have long debated what privacy should entail or whether it even exists in our society. As technology improves every year, the barriers that formerly defined private life from public become more blurred. In addition, not only do technological enhancements create problems in defining privacy, legislation, such as the Freedom of Information Act, also causes further difficulties. The average person would find defining privacy to an exact meaning perplexing, if not impossible. Yet most Americans would probably understand privacy as some form of secrecy kept to one's self. Of course, privacy entails a realm of human conduct that is "no one's business," except for those players involved who hold an immediate interest. Unfortunately, this definition can encompass a variety of issues both

in the public and private realms.[15] In a world becoming smaller each day, the exact meaning of privacy should be something both a layperson and a scholar can agree on, especially in understanding legislation; otherwise there arises the risk of conceptual confusion between society and the elite.

Judith Wagner Decew's book, In Pursuit of Privacy, discusses the many definitions of privacy. Essentially, privacy is a reference to "the separation of spheres of activity, limits on governmental authority, forbidden knowledge and experience, limited access, and ideas of group membership, to name a few possibilities." (Decew 1997, 13) As one can see, privacy encompasses a broad number of areas; thus finding a precise definition for privacy becomes a challenge. One possibility given is that it is the ability to make independent and self-legislating choices. (Decew 1997, 40) While this tends to be the major underlying idea in most constitutional cases, which usually hold some interest in making fundamentally independent, personal decisions, the real question is whether privacy entails more than just autonomy. The simple answer, according to the courts, is "yes," especially in regards to electronic surveillance, which has very little to do with autonomous decision making, and more to do with informal documented knowledge.[16] Privacy itself is a multifaceted concept where competing claims and values clash. However, this discussion will be limited to personal information acquired illegally or unethically through technological advances.

---

[15] In respect to the law, the public realm can sometimes include damages against private individuals, which would then fall under tort case law. Thus, the public realm would consist of whether or not the government has constitutional claims against an individual.
[16] In reference to informal documented knowledge, we shall also include private electronic mail, as well as information about Internet surfing.

Privacy's Evolution

Historically, it has been argued that the concept of privacy existed before the founding of the New World, dating as far back as the ancient Greeks. (Decew 1997, 9-25) Examples of the notion of privacy can be taken from philosophers such as Aristotle. The *polis*, as Aristotle discussed, was a structured political sphere where government and the city-state prevailed. By nature, man was a political creature and thus suited to participate in the political realm. Yet for Aristotle, in order for each man to hold an enviable status in the *polis*, he must first be master of his own private sphere, or *oikos*. The *oikos* involved the private household, or home, and the family life. This included concepts such as reproduction, birth, death, and other activities, which were either religious or what was "deemed individual," areas that were not available for public governance. (Decew 1997, 10; Swanson 1992 2-4) As one can see, the concept of *oikos* versus the *polis* is just the beginning of a long debate regarding communal interests against that of the individual.

In the United States, scholars contend that the Founding Fathers had intended for citizens to have some form of privacy when they wrote the Third[17] and Fourth[18] Amendments to the Constitution. (Scott 1995, 32-33) Furthermore, the additions of the First,[19] Fifth,[20] and Ninth Amendments,[21] "demonstrated an awareness that governments

---

[17] "No soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."
[18] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
[19] "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of

could threaten the privacy and integrity of each person and of his or her religious practice, speech, association, home, and personal possessions." (Strum 1998, 197) The origins of these amendments derived from the idea that each man was free and the master of his own castle. Thus, for a government to intrude upon that man's home or his liberty meant that the government was intruding into that man's personal privacy realm.

At the birth of this country, the colonials, who had lived in oppression under British rule and had suffered from the exploitation delivered through the hands of the British soldiers, sought to make their new government less intrusive and controlling. (Scott 1995, 42-43) Consequently, the tone of the Constitution, coupled with the new idea of federalism, began to shape this new nation. However, it was the combination of the Constitution and its amendments as well as the topography of the country that created an early decentralized government and a less communally oriented society, which sought and revered individuality. Arguably, the amendments to the Constitution can be called the chrysalis of the privacy arguments that we hold today.

The 1850s brought forth the beginning of actual documentation and awareness in the realm of emerging privacy rights. (Scott 1995, 37; Warren and Brandeis 1890, 207-210) It was a time when rugged individualism clashed with traditional society's knowledge of

---

the people peaceably to assemble, and to petition the government for a redress of grievances."

[20] "No person shall be held to answer for capital, or otherwise infamous crime, unless on presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

[21] "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

its neighbors.[22] Advancements in technology sparked an increase in the output of the media. Prior to the Civil War, there were few newspapers, primarily due to the expense of producing them. However, with the development in new technologies, such as the improvements in printing, photography and telegraphy, and the growing mass market of new, ill-educated readers (immigrants), newspapers felt the need to meet the market's demands. Between 1850 and 1890, the production of newspapers in the larger cities shot up from around 100 newspapers circulating to 800,000 readers a day, to approximately 900 urban papers with over 8 million readers. (Scott 1995, 38)

The outcomes of this new market were remarkable. Just about anyone who wished to know about newsworthy information could easily access it if he could read or have the paper read to him. No longer did a person have to hear a garbled story by word of mouth; he could access the story through an assumed reliable source. Moreover, this new form of journalism, which resulted from the increase in papers, also provided entertainment for the reader, presenting the news in a vivid and titillating way. This form soon came to be known as yellow journalism.[23]

As with all advancements in technology, the downside of these advancements allowed for the media to present pictures of private citizens and public figures easier than

---

[22] Looking over the history of humankind, traditional society stems from the idea that humans, at one time, lived together for the benefits of communal living that included security, a sense of belonging and an interdependency that included division of labor among the different members. In this society, being a member of the group overrode any sense of the independent self, thus privacy was not an issue. One did not have secrets from a neighbor. Even what would be considered private family information today, such as child rearing, was within the traditional community's knowledge and interests. (Scott 1995; DeCew 1997)

[23] The term yellow journalism originally resulted from the newspapers' yellowish tint, but later became known for the type of publication that focused on the upper echelon of

before. Soon blaring headlines and accompanying pictures sparked the acknowledgement that there was a threat to privacy. For example, in the 1890 New York case Marion Manola v. Stevens & Myers, "a starlet who was appearing wearing tights in a Broadway play became angry when two photographers secretly photographed her during her performance, one with a flash. Afraid they would take her photo to the newspapers, she sued to prevent them, and the New York Supreme Court agreeably complied, by issuing an injunction." (Scott 1995, 39) It was cases similar to this one, as well as the increasing aggressiveness and impropriety of the media, that led to a ground breaking article on privacy written by Samuel Warren and Louis Brandeis in the December 15, 1890 Harvard Law Review.

In their article, "The Right to Privacy," Warren and Brandeis discussed how, at the time, there was no clear conception of privacy in American law, even though there had been occasional references to the idea that people had the "right to be let alone." (Warren and Brandeis 1890, 193) They drew the examples for their arguments from cases in Britain and Ireland, as well as from philosophical arguments they conceived. They argued that the legal system needed privacy torts so that people could seek justice and compensation when their personal privacy was invaded. The villain throughout their argument was the irresponsible press that had run wild. It was their view that people living in this modern and complex life needed a "retreat from the world" through privacy and solitude. (Warren and Brandeis 1890, 196) But as a result of the invasiveness of the press, they doubted this ability to achieve peace of the soul or the private self. In the end, they believed that the individual should have the ability to determine his or her own mind

---

individuals as well as the criminals of the day. It was an eclectic mix of "sin, sex and

and to what degree he or she would communicate those thoughts to others. While most people of the time accepted this concept under a common law notion, Warren and Brandeis solidified this principle in their argument, which would play an important role in future Supreme Court cases.

The end of the nineteenth century and the beginning of the twentieth century brought additional confrontations between the press and private citizens. Yet what few people seemed to notice was the increasing intrusiveness of the United States government, especially in terms of electronic surveillance. By the 1920s, government surveillance became the new front in the battle against an individual's privacy. Eventually, this would become a fight over the privacy rights implied in the Fourth Amendment. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." However, the government argued that as long as the surveillance did not invade or intrude into a suspect's home, it had followed the letter of the law. While the Supreme Court did not always agree with the government on the issue of intrusiveness, it would not be until the 1960s that the Court would reprimand the government for violating an individual's space.[24]

The 1960s brought forth a plethora of privacy dilemmas, ranging across an individual's autonomy in decisions regarding her own reproductive system, government

---

violence" and fit today's view of the news. (Scott 1995, 38)

[24] See Silverman v. United States, 365 U.S. 505 [1960].

warrantless wiretapping, an individual's refusal to cut his hair, the rights of high school students, and the right to observe or read obscenity in the privacy of one's own home. (Gottfried 1994, 104-105) Some of these issues, as discussed previously, had more to do with an individual's autonomy and that of the state's interest. However, a growing number had to do with emerging new technologies, which allowed for more government intervention. In addition, American society was characterized by an increase in antiestablishment political thinking which was reflected in the mid-1960s counterculture. Furthermore, the explosion in surveillance technology not only came from the government, but also from the private corporate sector. (Scott 1995, 53)

As society began to feel the emergence of privacy rights, traditional monitors, such as the family, the education system, and religion started to erode. The social constraints and relationships that once dictated the morals and feelings of accountability to others no longer mattered as much and the notion of the individual began to root itself within the culture. As a result, the government began to grow, taking the place of the traditional behavior controlling mechanisms, and becoming the dominating factor in deciding upon acceptable behavior in society. For example, the government began to address issues involving discrimination and the right to work, reproduction, abortion, copulation between two consenting adults, and child labor to name a few. (Blank and Merrick 1995) In addition, once people began to isolate themselves as individuals from the group, curiosity about information on those people that at one time might have been easy to come by, rose. The outcome was an increase in the public's demand for information on other people and in the behaviors of those people, which, as discussed, were no longer being monitored by traditional elements in society. Unfortunately this demand for

knowledge on another's life has been one of the contributing factors that have led to the problems that people are facing today, such as the fascination with public figures' private lives and problems. (Scott 1995, 54)

America's Constitutional Privacy

One of the best methods for defining privacy and its history in America is seen in numerous Supreme Court opinions throughout the years. The very first Court opinion on personal privacy against governmental intrusion can be seen in the 1889 case of Boyd v. United States. This landmark case in privacy protection involved the importation of plate glass and the lack of duty payment by E. A. Boyd & Sons to customs as dictated by the then current customs act. The district attorney, acting under the authorization of the customs act, obtained a court order for the invoices pertaining to the Boyds' plate glass. In response, the Boyds argued that the compulsory production of their files violated their Fourth and Fifth Amendment rights in respect to the prohibition of unreasonable search and seizures as well as their right to protect themselves from self-incrimination.

The United States Supreme Court upheld the Boyds' argument with two justices dissenting on the grounds of the Court's Fourth Amendment argument. Justice Joseph Bradley for the Court opined that:

> The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach further than the concrete form of the case...they apply to all invasions on the part of the government and its employes [sic] of the sanctity of a man's home and the privacies [sic] of life. It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty. [sic] and private property, where that right has never been forfeited by his conviction of some public offense,- it is an invasion of this sacred right which

> underlines and constitutes the essence of [the] judgment. (Boyd and others, Claimants, etc. v. United States 116 U.S. 532 [1886])

Yet it was not until the 1928 case of Olmstead v. United States that the Court had a chance to readdress the argument for personal privacy against government intrusion. During this era, the United States had passed the National Prohibition Act, and Olmstead was convicted of the transporting and selling of alcohol. He appealed to the Court on the grounds that the evidence was illegally obtained through a wiretap. The Court found that privacy had not been invaded under the Fourth and Fifth Amendments as Olmstead had contended, since there was no physical invasion of his house. Furthermore, Chief Justice William Taft held that conversations between two private individuals were not protected by the Fourth Amendment. Thus, for the moment, the Court upheld the government wiretap. However, in one of the most famous opinions on privacy ever written, Supreme Court Justice Louis Brandeis' dissent stated:

> The protection guaranteed...is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of a man's spiritual nature, of his feelings and of his intellect...They conferred as against the government, the right to be let alone- the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by government upon the privacy of an individual, whatever the means employed, must be deemed as a violation of the Fourth Amendment. (Olmstead v. United States 493 U.S. 572 [1928])

Despite Brandeis' comment, the Court would continue to side with the government until the passage of the 1934 Federal Communications Act, which prohibited the interception or retransmission of any communication intercepted via wire or radio. (U.S. Public Law 416, Sec. 605)

Shortly after the passage of the 1934 Federal Communications Act, the case of Nardone et al. v. United States began to change the definition of privacy and the areas of

its protection. Frank Carmine Nardone and others, like Olmstead, were also convicted of smuggling alcohol. Their dealings had been obtained through a wiretap via federal officers. Nardone contended that the evidence procured by the federal officers' wiretap was inadmissible due to the 1934 law. Justice Owen J. Roberts, writing for the Court stated: "Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty...wiretapping by officers...involves a grave wrong."(Nardone et al v. United States 302 U.S. 277 [1937]) As a result, this case became one of many that would weaken the Olmstead decision and strengthen arguments on personal privacy against government intrusion. However, the courts would continue to hold, until 1967, that in wiretapping cases, the Fourth Amendment could be applied only when there was physical entry and seizure of tangible items. Overheard conversations, at this point, were still unprotected.

By the 1960s, the adopted argument on privacy was that the right was a derivative of some of the other constitutional rights, as pointed out in Griswold v. Connecticut, 381 U.S. 479 at 486 (1965). It was argued that these rights not only included property rights, but also rights to "bodily security," which have very little to do with the people who are not the main actors in a specific situation. (Decew 1997, 46) As Justice William O. Douglas said in this case on contraceptives, " [w]e deal with a right of privacy older than the Bill of Rights- older than our political parties, older than our school system...It is an association that promotes a way of life, not causes; a harmony in living, not political faiths; a bilateral loyalty, not commercial or social projects." (Griswold v. Connecticut, 381 U.S. 479 [1965]) Government must be limited in some realms, Douglas wrote, as the

Supreme Court struck down the Connecticut law forbidding the counseling or use of contraceptives by anyone in the state.[25] While this may have little to do with electronic surveillance, this decision is important because it not only broadened the realm of privacy but also strengthened the base for this right. In this case, the holding rested upon the due process clause of the Fourteenth Amendment, as well as in the "penumbra" of privacy interests protected in the First, Third, Fourth, Fifth, and Ninth Amendments.

The case that arguably overturned what little was left of Olmstead was Katz v. United States(1967). Katz was convicted under an indictment that charged him with transmitting wagering information through the telephone across state lines. This was a violation of 18 U. S. C. 1084. Government agents had attached an electronic listening and recording device to the outside of his most frequented telephone booth and had proceeded to document his unlawful transgressions. The Court held, as stated by Justice Potter Stewart, that the Fourth Amendment is not to be translated as a general "right to privacy." The Amendment "...protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy...[it is meant to] protect people, not places." (Katz v United States 389 U.S. 350-351 [1967])

Moreover, he wrote that if a person knowingly exposes information to the public, then it is not covered by the Fourth Amendment. "But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected...[W]hat he sought to exclude when he entered the booth was not the intruding

---

[25] However, the legitimate concern of others can vary according to the circumstance involved and the culture. For example, in the United States, a couple's decision about whether or not they use contraceptives is beyond the concern of others, yet in countries such as China or India, this "governmental intrusion" or concern plays a legitimate role in the population problems that they face today. (Decew 1997, 56)

eye- it was the uninvited ear..."(Katz v United States 389 U.S. 350-351[1967]) Therefore, as Stewart contends, an individual who seeks privacy in a telephone booth may rely upon the protection of the Fourth Amendment. Once the person enters the booth, shuts the door so as not to be overheard, and pays the toll, he or she is entitled to the idea that whatever is said into the receiver will not be available to the world's inquisitive ears. Hence the government agents ignored what Stewart called "the procedure of antecedent justification," which is instrumental in the Fourth Amendment. (Katz v United States 389 U.S. 359 [1967]) This procedure is a required constitutional precondition due to the type of electronic surveillance that was used, as discussed at length in a previous case.[26] Since the surveillance in this case failed to meet the required precondition, the case was reversed.

What resulted from this case was that the courts had significantly changed the approach they use in determining whether or not searches and probable cause allowances violated the nature of the Fourth Amendment. This approach came to be known as the privacy test. No longer were the physical boundaries of the home the only area that was private, but the conversations between individuals over the phone, regardless of the telephone's location, were covered as well, as long as the individuals sought privacy from society.[27] In Justice John Harlan Marshall's concurring opinion, he discussed this two-pronged privacy test that the courts had developed loosely in relation to what locations qualify as areas of presumed privacy protection. The first requirement was that a person

---

[26] This constitutional precondition is discussed more in Osborn v. United States, 385 U.S. 323, 330 [1966] (Katz v United States 389 U.S. 362 [1967])

[27] This understanding of privacy is not only limited to telephone conversations, but also includes other aspects of life, which would arguably be deemed more personal.

had to exhibit an expectation of privacy, even though it was a subjective expectation. The second requirement was that society recognized this expectation as "reasonable". (Katz v United States 389 U.S. 361 [1967]) Some have contended that it is extremely difficult to meet the first requirement, since the government can socialize its citizens on the areas that can be considered private or it can manipulate the law surrounding areas which could be deemed private by another society. The second requirement is just as difficult in that it is subjective to the beliefs of society or those who interpret those beliefs-- the government.

By 1968-1969, the government received a formidable blow for once again engaging in improper electronic surveillance. In Alderman v. United States, Ivanov v. United States, and Butenko v. United States, the petitioners were convicted of conspiring to transmit murderous threats in interstate commerce. They had discovered, after their convictions and first appeals, that their place of doing business in Chicago had been subject to electronic surveillance by the government. The Supreme Court held that the government was required to turn over all illegally obtained surveillance material to the defendants, whose Fourth Amendment rights had been violated. As discussed in Katz, the Fourth Amendment afforded privacy protections against the "uninvited ear.... [Therefore,] oral statements, if illegally overheard, and their fruits are also subject to suppression." (Alderman et al v. United States 394 U.S. 171[1968]) The Court stated that the suppression of evidence obtained in violation of the Fourth Amendment can be only by those individuals whose rights were violated by the search.[28] Furthermore, after

[28] "In order to be a 'person aggrieved by an unlawful search and seizure' one must have been a victim of a search or seizure, one against whom the search was directed, as distinguished from one who claims prejudice only through the use of evidence gathered

the defendants receive the illegally-obtained material, they have the right to examine the information to determine what parts the government may use in building its case. This allows the defendants to build a case challenging the information that the government already has. While this seems unfair to the government, the objective was to allow only official eavesdropping and wiretapping obtained through probable cause and a warrant.[29] "Nothing can destroy a government more quickly than its failure to observe its own laws, or worse, its disregard of the character of its own existence." (Alderman et al v. United States 394 U.S. 202[1968])

Since the 1968 Alderman decision, the courts have wavered between the government's right to know and that of the individual's right to privacy. The most recent case, seen in 1998 in the district courts, is Timothy R. McVeigh v. William S. Cohen, et al.[30] Timothy McVeigh was a highly decorated noncommissioned officer who was the highest- ranking enlisted person aboard the USS Chicago, a nuclear submarine. On September 2, 1997, a civilian Navy volunteer received an electronic mail message via the America Online Service Provider (AOL) regarding a toy drive that she was coordinating for the submarine crew's children. She noticed that the message box stated that the e-mail had originated from the alias "boysrch," but the text was signed "Tim." Using the "member profile directory" option on AOL, she discovered that the subscriber was named Tim, lived in Honolulu, Hawaii, worked in the military, and identified his marital

---

as a consequence of a search or seizure directed at someone else..." (Alderman et al v. United States 394 U.S. 173[1968])

[29] "In 1979, ...the Court held that because Congress must have recognized that most electronic bugs can be installed only by agents who secretly entered the premises, warrants authorizing such surveillance need not explicitly authorize covert entry." (Biskupic and Witt 1997, 588)

[30] Timothy McVeigh is no relation to the convicted Oklahoma City bomber.

status as homosexual. Included in this profile were his listings of favorite activities, which included "collecting pics of other young studs" and "boywatching." What the profile lacked were his full name, address, and phone number. After discovering this information, the volunteer proceeded to forward this information to her husband, who was also a noncommissioned officer aboard the USS Chicago. Eventually, this material found its way to the captain of the ship, who was McVeigh's commanding officer. At this point, the ship's legal advisor was called in to investigate suspicions that Timothy McVeigh was in fact the "Tim" listed under "boysrch." Formal investigations began, and the investigator instructed a paralegal assistant to contact America Online to get account information on the identity of "boysrch." Without identifying himself or providing a warrant, the assistant led the AOL representative to believe that he was an associate of McVeigh's, and that he was following up on a previously sent fax from the company, and needed verification of the handle "boysrch." The AOL representative identified the handle to be Timothy McVeigh. McVeigh was then informed that he had violated the military's policy of "Don't Ask, Don't Tell, Don't Pursue."[31] The Navy conducted an administrative discharge hearing, using the e-mail as its major form of evidence. The decision ordered McVeigh's discharge from the Navy, but the day prior to his discharge, he filed suit to win an injunction from the district court to block the discharge. (Timothy

[31] The "Don't Ask, Don't Tell, Don't Pursue" policy was created under the National Defense Authorization Act of 1994. This policy applied to homosexuals serving in the military. This policy was the result of a political compromise, which allowed homosexuals to continue serving in the military as long as they did not disclose their sexual orientation to any person. In return, the military would not go out of its way to seek out, and discharge, homosexuals. (Timothy R. McVeigh v. William S. Cohen, et al., Civil Action 98-116, United States District Court for the District of Columbia 1998)

R. McVeigh v. William S. Cohen, et al., Civil Action 98-116, United States District Court for the District of Columbia 1-3 [1998])

The district court found that McVeigh's anonymous e-mail was not an admission that should trigger an investigation under this policy. Furthermore, Judge Stanley Sporkin held that the Navy had violated the Electronic Communications Privacy Act of 1986 [18 U.S.C. §§ 2073(b) (A)-(B), (c) (1) (b)]. He wrote that the Electronic Communications Privacy Act (ECPA) declares that government can obtain information from an ISP, "only if a) it obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent; or b) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question." (Timothy R. McVeigh v. William S. Cohen, et al., Civil Action 98-116, United States District Court for the District of Columbia 4-5 [1998]) In this particular case, the Navy had failed to comply with either of these procedures. Moreover, Sporkin asserted that the government knew or should have known that AOL was breaking the law by turning over the information without a warrant, despite the fact the Navy solicited the information. Accordingly, McVeigh's injunction was granted.

While this case does not address whether the "Don't Ask, Don't Tell, Don't Pursue" policy is constitutional, it does address a privacy issue. Not only does it affirm the ECPA and the privacy rights of users on all ISPs, but it also reinforces the Supreme Court's decision in Alderman stating that "information obtained improperly can be suppressed where an individual's rights have been violated. In these days of 'big brother,' where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting

these rights be observed." (Timothy R. McVeigh v. William S. Cohen, et al., Civil Action 98-116, United States District Court for the District of Columbia 5 [1998])

Of course, over the twentieth century there have been several more cases in the court system that continued to expand and redefine privacy in respect to electronic surveillance.[32] The main conclusion one arrives at is the Court's sanction against government intrusion in a new technological realm. Furthermore, the Court's disapproval of the invasion of privacy using technological advancements has been seen over and over in many of these cases. In fact, one could argue that the courts would turn a blind eye to some undesirable actions, as long as the constitutional right of privacy for those prosecuted were not infringed upon. However, while courts have tended to hold a broad privacy position, especially in respect to the Fourth and Fifth Amendments, Congress and executive agencies have begun in their own ways to chip away and redefine, as well as violate, the courts' privacy decisions.

[32]Such examples include, but are not limited to the following cases: United States of America v. Jake Baker and Arthur Gonda CR95-80106 [1995], and United States of America v. Robert Alan Thomas and Carleen Thomas Civil Action 94-6648 & 94-6649, U.S. Court of Appeals [1996]. (See Footnote 34 for more examples)

CHAPTER III

UNCLE SAM LEGISLATES

As discussed in Chapter Two, over the years the federal court system established groundbreaking precedents in the controversial realm of government intrusion versus citizens' rights.[33] While the federal courts have defined the boundaries of privacy in terms of government involvement and the "right to be left alone" (Warren and Brandeis 1890, 193), the legislature has found difficulty creating law that balances the Supreme Court's decisions and those of the state's police and intelligence surveillance interests. This chapter will examine the legislature's attempt at integrating these two opposing interests and discuss the legislative protection of privacy and its implications or effects in the realm of cyberspace.

Privacy in the Legislature

The realm of privacy in an era of advanced technology was not addressed in the United States Congress until the early part of the twentieth century. One reason the

[33] While this argument tends to deal with privacy in the aspect of information about one's self, government intrusion, and eventually the relation to the Internet, there are many other aspects of privacy that do not relate to electronic surveillance or the Internet. Unfortunately some of those cases were not decided in the interests of the person's privacy interests, i.e., California Banker's Association v. Schulz (1974), United States v. Miller (1976), Oliver v. United States (1984), Bowers v. Hardwick (1986), California v. Greenwood (1988), O'Connor v. Ortega (1987), and Florida v. Riley (1989).

Congress began to address privacy, as stated in Chapter Two, resulted from the tensions between society's diminishing role as a behavior-modifying agent, the rise in the individual's sense of self, and the government's emerging role as the new moral controlling mechanism. In traditional society, privacy was not an issue simply due to the involvement in the community overrode those interests of the self. A person was far more interested in being involved in the community for safety or security reasons, as well as for social interactions with others, such as to reproduce. Therefore, the whole community was aware of almost every aspect of a person. Many characteristics about a person and much of that person's history were community knowledge. Today, many American citizens would deem this previous community knowledge as infringements upon an individual's private life. However, it would not be until the population increase in migration to larger cities took place that the emergence of personal privacy realms would come to exist.

In America, not only did immigration to the cities lead to increased awareness of privacy, due to the ability to become anonymous and therefore private, but also as many Americans began to move west, the societal pressures of traditional communal environments began to lessen. In short, neighbors knew less of one another due to their physical separation from the community by large tracts of land. This increase in a lack of knowledge about one's neighbor, as well as advocating the privacy of the individual, in fact intensified the concepts of personal privacy and their breaches under the increasing intrusions committed by the growing media and inquisitive law enforcement bodies. Legal remedies for the offended would begin to take shape once the courts began to act in this area where the Congress would not.

One of the first laws to be created in protecting new technology and the citizens' right to privacy against government intrusion was the Communications Act of 1934.[34] The original intent of this statute was to regulate interstate and foreign communications that traveled by radio wave or through cables/ wire (i.e., the telephone). As discussed in section 4 of the law, the newly established regulating body became known as the Federal Communications Commission (FCC). The law also discusses the licensing of radio communications and transmissions (Title III), FCC's jurisdiction, government owned stations and those of foreign vessels, and the allocation of facilities. Furthermore, provisions for antitrust violations, establishing lotteries and announcements over the air waves, operating and construction permits, distress signals and communications, censorship and indecent language,[35] the employees of a communication facility, third parties, and the government are addressed as well.

The most important aspect of this law, in terms of protected privacy for communication such as the Internet, is section 605. This section discusses the unauthorized publication of communications. It explicitly states that:

> No person receiving...any interstate or foreign communication...shall divulge or publish the existence, contents, substance...or meaning thereof...to any other person other than the addressee, his agent, or attorney...or in response to a subpoena issued by a court of competent jurisdiction... [Moreover,] no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance...or meaning of such intercepted communication to any person. (U.S. Public Law No. 416 Sec. 605)

---

[34] This law is known as U.S. Public Law No. 416

[35] In respect to some free speech advocates who argue against the Communications Act, section 326 of this act supports many of their arguments stating that "[n]othing in this Act shall be understood or construed to give the Commission power of censorship over the radio communications or signals transmitted by any radio station, and no regulation or condition shall...interfere with the right of free speech by means of radio communication." Unfortunately it also gives the provision that no person can utter obscene, indecent, or profane language over the radio.

In this excerpt, "person" is defined as an individual, an association, a corporation, or a trust. However, in its implication, as used by the courts in Nardone et al v. United States, a person can also be a government agent. Thus the actual meaning of the law implies that the government, as a third party, cannot interfere with or intercept a private communication between two individuals over a telephone line. As stated in Nardone, the plain words of this section forbid anyone who is not the sender or the sender's authorized person to intercept or divulge a communication that took place over the telephone lines.

One can argue about the meaning of this law in relation to its applicability to law enforcement officials, as interpreted in Nardone. However, the question of whether Congress meant to include the government and its right to protect the nation is debatable. The two questions at hand that involve this law are whether the sovereign is deprived of a recognized or established principle or prerogative if this act includes them, or whether it implied that the sovereign or its officials are excluded from the language of the law that embraces all people regardless of occupation. Today, as in the late 1930s, one can look at the history of Congress to decide their intent. Even though the members of Congress had realized that the language neglected to be specific in matters concerning the government's interception, one can see that they sought to remedy the situation by introducing bills that would limit the government and its agents' use of wiretapping for criminal convictions. (Nardone et al v. United States 302 U.S. 276 [1937]) While none of the amendments to the bill ever mustered enough support to change the document, the realization by many members of Congress and the numerous attempted corrections of that mistake was made enough times for the courts to make judgment on this issue.

In respect to the Internet, this law establishes protection against government monitoring of e-mail, Internet surfing, and Internet phone calls. However, because of the dial-up process and the need for an ISP in order to access the Internet, this law does not forbid employees of ISPs from viewing a patron's e-mail or the detailed layout of web pages visited. The reason, located in Sec. 605, behind this employee access are the exemptions concerning the, "assisting of receiving" or "assisting of transmitting" communication phrases. Furthermore, in later privacy cases against employers, employees found that this clause also permitted managers to view their e-mails since it involved an aspect of the employees' work performance and production. (Alana Shoars v. Epson America, Inc., No. B 073234, Los Angeles Superior Court. [1990]) The main issue to understand, though, is that third parties not related to the transmitting or receiving of a certain communication, cannot view private communications or access them. As seen in earlier judicial decisions, this plays a major role in the government's ability to intrude upon an individual's right to Internet privacy.

The Communications Act of 1934, as interpreted by the Supreme Court, can be seen as the groundwork in privacy legislation for the Internet. However some critics, e.g., organizations such as the Ethical Spectacle and the Center for Democracy and Technology, have argued that it is by far one of the worst written laws, as discussed in articles such as "The Communications Act of 1934 Was a Mistake." (Ethical Spectacle 1996, 1) However, most of their criticism is against section 326 of the law, which discusses censorship and indecent language. It states in two sentences that the FCC cannot censor anyone, yet no one can utter any "obscene, indecent or profane language by means of radio communication." (U.S. Public Law No. 416 Sec. 326) In respect to the

Internet, one could argue that the FCC, as a government established body, could invade a Netizen's right to privacy, through the interception of e-mail only for the sake of enforcing the obscenity clause of section 326. In addition the amendments made to the Communications Act of 1934 by the Communications Decency Act are the main points of contention seen in today's freedom of speech arguments.

As seen implicitly in the previous chapter through the increase in judicial activity, in the late 1960s, there was a growth in government surveillance techniques, as well as government intervention in what could be termed as private realms.[36] With the courts favoring personal privacy over government intervention, the Congress and the public became increasingly aware of law enforcement's use of electronic surveillance techniques. In addition, the Communications Act of 1934 did not cover all privacy interests. Congress later felt that the federal collection, use, and dissemination of personal information affected the privacy of the individual citizens. Coupled with the increasing use of computers and new technology, not to mention the possible misuses of that information, they believed that citizens faced an increased harm, and that their protections were in danger.

As a result, Congress passed the Privacy Act of 1974, also referred to as Public Law 93-579. Embodied in this act were the 1964 Freedom of Information Act's principles and the 1972 Advisory Committee on Automated Personal Data Systems to the Secretary of the Department of Health, Education, and Welfare's response to the public's and the legislature's concern that the government was turning into "Big Brother." The committee

---

[36] See footnote 33 for other government intrusions, as well as Timothy R. McVeigh v. William S. Cohen, et al., Civil Action 98-116, U.S. District Court for the District of Columbia [1998]

suggested five principles that it believed would protect privacy from Big Brother and the developing little brothers in this new information age.[37] These principles state that:

> There must be no data record-keeping systems whose very existence is secret. There must [also] be a way for an individual to find out what information about him/her is on record and how it is used. [Moreover, there] must be a way to correct or amend a record of identifiable information about him/her. [Additionally, there] must be a way for an individual to prevent information about him/ her that was obtained for one purpose from being used or made available for other purposes without his/her consent. [And finally, any] organization creating, maintaining, using, or disseminating records of identifiable personal data must guarantee the reliability of the data for their intended use and must take precautions to prevent misuse. (Henderson 1999, 19)

Eventually these five principles would also be the foundation for the Electronic Privacy Act of 1986.

In the Privacy Act of 1974, not only was the purpose of the act to protect the five principles mentioned before, but also to allow for a sixth principle which stated that there had to be a way for a person to bring civil suit for any damages incurred as a result of willful or intentional actions. (U.S. Public Law 93-579, 42-43) Consequently the act provided for the accountability of federal agencies and private corporations on certain disclosures, the accessibility of records, federal agency requirements and rules, civil remedies, and criminal penalties and exemptions. The act also went so far as to cover the actions or rights of legal guardians, archival records, mailing lists, and sanctions against the government. Unfortunately, while the citizen's privacy became more protected from the federal government, the act still neglected to cover the privacy rights guaranteed from

---

[37] Little brothers are corporations or companies who collect data on individuals for business uses. Eventually, this data would be collected, sold, or exchanged to other companies, who could in turn keep extensive dossiers on an individual's personal life, knowing their shopping preferences, taste in food, their yearly income, and what they owned. (Henderson 1999, 19)

private corporations as seen in section 5, subsection 522a (m) (2). (U.S. Public Law 93-579, 50)

While this act initially sought to help citizens learn about the information collected on them and how to correct and protect that information, many critics, such as the American Civil Liberties Union (ACLU), have found this act useless due to poor implementation and the lack of enforcement. Furthermore, problems with the act are exacerbated since there were no appropriated funds for the enforcement of provisions relating to privacy. As a result, most government agencies did not bother to appoint people to oversee privacy implementation. The Office of Management and Budget (OMB), which originally was appointed this task of privacy enforcement because no other agency would volunteer to act as the enforcing agency, found it could not fulfill the required enforcement in conjunction with its other duties. After privacy enforcement by the OMB failed, no other federal agency volunteered to become the enforcer for privacy. Thus, without the enforcing bodies to define the terms of the law and penalize lack of compliance, agencies became their own judges of whether or not they fulfilled the requirements of the law correctly. (Strum 1998, 159-154)

Nevertheless, some critics, such as Harry Henderson, still contend that, while cumbersome, the Privacy Act of 1974 does provide citizens with legal remedies should they suspect the government has inappropriate or inaccurate information about them, or has distributed that information maliciously. That person need only determine which agency has the information and then request it. The only exceptions to their inquiries on their own information would be files located in law enforcement agencies or intelligence agencies. (Henderson 1999, 33)

Following the 1974 Privacy Act and the Freedom of Information Act, there was a plethora of privacy legislation that was passed in the 1980s. One of the first pieces of legislation was dubbed the Privacy Protection Act of 1980.[38] This act stipulates when searches are authorized, as well as who is allowed to perform them.[39] The prominent themes in this document are the requirement of warrants and the principles of the 4th Amendment. In essence, law enforcement cannot perform searches or seize any "work product" or "documentary material" without a warrant. (U.S. Public Law 96-440, section 42 U. S. C. 2000aa (a)- 2000aa-11 (a) (4) 95-99) Materials can be seized only if there is probable cause to believe that the person possessing the material is involved in a crime and the material is evidence of this crime or may relate to national security. This includes materials intended for publication by journalists and publishers in the preparation of newspapers, broadcasts, books, and other types of public communications.

In addition, this act forces law enforcement to utilize subpoenas and citizen cooperation to obtain evidence in respect to First Amendment activities. As in previous acts, this statute also provides for legal compensation for damages should a government agent, following the orders of his/her agency, violate any portion of this law and wrongly seize an item or search an area. The implication provided in this body of work is that protection of private documents or information can extend to materials intended for publication on online systems as well as electronic bulletin board systems (BBS).

One criticism of this act relates to section 2000aa-12. This section discusses the binding nature of the guidelines discussed in the bill, as well as disciplinary action and

---

[38] Also known as U.S. Public Law 96-440.

[39] Only those involved in the investigation can do the searching and if need be the seizing of items.

the legal process for noncompliance with the law. In two rather long sentences that seem to contradict the earlier provision in section 2000aa-6, it states that the violation of the guidelines would subject an employee or an officer only to administrative disciplinary action. Furthermore, if the issue is related to compliance or the failure to comply, there can be no litigation, and the court cannot suppress or exclude evidence. What one could argue is that, hypothetically, if an enterprising officer, who fails to obtain a warrant, decides to seize information due to his concern that if he did not there might be a breach of national security or someone would incur bodily harm, the victim of his search could not bring legal suit against the officer for seizure of his/her items. Moreover, if the officer is correct in his assumptions, he might receive slight disciplinary action, such as a verbal warning, but cannot be held criminally or civilly liable. However, the agency can be held liable depending upon the violation.

While one could argue the slippery slope implications of this provision and how, in the wrong hands, the government would not be held accountable for much, this act has in fact helped some victims reclaim seized items from the government. In the case of Steve Jackson Games, Inc. v. United States Secret Service, the Secret Service organized an investigation into the hacker group called the "Legion of Doom." Their belief was that the organization had stolen confidential information about the emergency Bell South 911-phone system, which was actually available to the public for a few dollars, compliments of the Freedom of Information Act. Through much guesswork in their investigative processes, the Secret Service falsely assumed a computer BBS game system known as the

"Illuminati" was connected with another BBS, called the "Phoenix."[40] They believed the operator of the "Phoenix" BBS, Lloyd Blankenship, was an associate of the Legion of Doom, because the site happened to have the "confidential" manual on its board for downloading. They connected the "Illuminati," which was owned and operated by Steve Jackson Games, to the "Phoenix" BBS through Blankenship, who happened to be an employee of Steve Jackson Games. (Henderson 1999, 77)

On March 1, 1990, the Secret Service raided Steve Jackson Games and confiscated thousands of computer disks. In addition, they seized all computer equipment and files used by the company. The agents believed they struck pay dirt when they uncovered an alleged "how-to" manual for computer criminals. In actuality, the document in question was a rule book for a role-playing game that was being developed around the idea of a futuristic high tech society. (Henderson 1999, 77; Center for Democracy and Technology 2001, 1)

Steve Jackson repeatedly asked the Secret Service for the return of his seized items, after they had finished copying them, but the agency ignored his requests. His lack of business material for the game shop, which included the developed new games as well as the role/ rule books for current ongoing games, eventually forced him into bankruptcy. As a result Jackson sued the Secret Service. (Henderson 1999, 77)

The Texas District court found that, under the Privacy Act, the Secret Service had violated Jackson's rights. Furthermore, the judge noted, "while the content of these publications are not similar to those of daily newspapers, news magazines, or other

---

[40] This BBS did happen to have hacker-related conversation and material on it as well as the Bell South 911 information.

publications usually thought of by this court as disseminating information to the public, these products come within the literal language of the Protection Act." (Henderson 1999, 77) Jackson was awarded damages,[41] but the impact of both the case and the act were reflected in law enforcement's realization that privacy statutes, and First and Fourth Amendment rights had to be considered in the realm of computer communications and documents.

A small but significant and effective privacy act, which was born in the 1980s, was the Cable Communications Policy Act of 1984.[42] The act protects subscriber privacy by hindering cable operators or third parties from monitoring cable consumer buying and viewing habits. Likewise, it prohibits the collection of "personally identifiable information" (PII), unless authorized by the subscriber. (U.S. Public Law 98-549, section 47 U. S. C. § 551 (c) 101) The exceptions to this rule are if the PII is needed in order to render a service by the operator or the PII is needed to conduct legitimate business activity related to the service, for instance sending a bill. (U.S. Public Law 98-549, section 47 U. S. C. § 551 (c) (2) (A) 101) In addition the act places a heavy burden of proof on law enforcement agencies seeking court orders for consumer information. The implications of this bill are that it will extend to the new online services provided by cable companies, and that, eventually, this might allow for the protection of an ISP's members' PII against government intrusion.

The end of the 1980s brought the Electronic Communications and Privacy Act (ECPA) of 1986. The ECPA was an update to Title III of the Omnibus Crime Control

---

[41] Unfortunately this case still is unresolved, since the appellate court reversed the decision in favor of the government. (Center for Democracy and Technology 2001, 1)
[42] Also referred to as U.S. Public Law 98-549.

and Safe Street Act of 1968. Originally, Title III of the Omnibus bill regulated the use of government wiretaps and hidden microphones, requiring that the consent of one party be obtained prior to the tap and/ or that a court order be obtained. In addition, it prohibited wiretapping of employees by private parties or public investigators. Title III also established a procedure that requires a warrant authorizing electronic surveillance and the use of wiretaps. While Title III protected aural communication transmitted through wire or cables, it failed to protect e-mail content as well as communications over cordless telephones. Obviously this opened the door to unrestricted government electronic surveillance on wireless transmissions and non-aural communications such as e-mail and faxes. (Strum 1998, 141-142)

As mentioned before, the ECPA was an update to Title III of the Omnibus bill. This act not only protected previous communication technology, such as two-party phone calls, but also provided protections for all new forms of digital and computer communications. This included communications via video, electronic transmissions, text, data, and audio, which were all equated to that of a phone conversation within the home or that of first class mail.[43] Like the Communications Act of 1934, the ECPA included protections against interception and disclosure of communications. Furthermore, the sanctions in the ECPA applied not only to the government, but also to private companies and individuals as well. (U.S. Public Law 99-508 Sec. 2511) After the act became law, government was required to obtain a court order or the prior consent of one party before initiating any electronic surveillance through a wiretap, whether accessing real time

---

[43] This did not include cordless phones or tone only paging devices. (Strum 1999, 158; Rubinstein 1999, 3)

communications or stored messages. (U.S. Public Law 99-508 Sec. 2511 (2) (a) – (b) 107-108) Restrictions against private companies were reflective of the principles stated in the Cable Communications Policy Act and the 1934 Communications Act. As in those two previous acts, the only acceptable monitoring of communication by a third party, such as the service provider, was for information received and distributed in the normal course of business for providing a specific service, such as some sort of mechanical or service quality control check. (U.S. Public Law 99-508 Sec. 2512 (2) (a))

The advantages to the ECPA not only included those of broader protections for a growing realm of communication technology, but it also clarified invasions of privacy and codified protections against those invasions, as seen in Timothy R. McVeigh v. William S. Cohen, et al. in Chapter Two. In addition it sought to curb government surveillance and recreational eavesdropping, unless committed by an employee's employer in respect to work e-mail or business telephone communications.

The largest criticism of the ECPA came from the ACLU, which originally endorsed the act, stating that it protected civil liberties. Yet since the signing of the act into law, the ECPA has been ridiculed for its failure to protect and enforce certain electronic communication procedures. Moreover, critics have pointed to key discrepancies between the actual law and the original versions, which were promoted by civil libertarians. (Rubinstein 1999, 3)

One main contention lies within section 2516, which lists a host of prosecutable violations, including bribery, child pornography, counterfeiting, hacking inaccessible information and the transportation of stolen property. A critic from The Nation called this "a wish list for the law-enforcement community." (Rubinstein 1999, 3) Not only did

the ECPA substantially increase the list of federal crimes permitting the use of government electronic surveillance, but it also increased the number of Justice Department officials who can give judicial approval for court orders such as warrants. (U.S. Public Law 99-508 Sec. 2516 (2))

Critics also argue that ECPA provisions regarding access to certain subscriber information has been made easier for law enforcement agencies to obtain, since in certain instances there is no provision for judicial review. Requests for customer records from service providers need be accompanied only by a statement that certifies the information requested pertains to an investigation that involves the interception of foreign intelligence. (U.S. Public Law 99-508 Sec. 2511 (2) (e)- (f)) This easy accessibility enhances arguments questioning the certifying procedures of law enforcement officials and service providers, since the original intention of the ECPA was designed to protect communications. (Rubinstein 1999, 3)

Some final criticisms of the ECPA result from the revised definition of "content," which seems to exclude the existence of "communication," as well as the identities of the parties involved in the transmission. (Rubinstein 1999, 3-4) The actual text defines "contents" as "any information concerning the substance, purport, or meaning of that communication." (U.S. Public Law 99-508 Sec. 2510 (8)) However, the definition, as the critic Geoffrey Rubinstein has pointed out, lacks what is the expression of communication between two parties. What this may mean is that there might be a closer scrutiny of calling and e-mail correspondence patterns. In addition, after September 11, 2001, Americans have seen an increase in specialized surveillance programs, such as DCS1000, discussed in Chapter One. One could argue that the ECPA's 2511 provision

will eventually allow for full government surveillance of the populace, which would include monitoring political groups, student action committees, and even communities. To move further in the argument, even though government must apply for a wiretap in order to have access to the substance of a communication, a tap and trace would allow the government to define invisible social networks and identify key members within those social groups.

In 1996, Congress passed the Telecommunications Act. This act, resembling the Cable Communications Policy Act of 1984, dealt with the privacy of customer information and FCC implementation. In general, the act states that every telecommunications carrier has a duty to protect the confidentiality of information, not only relating to the customers, but also relating to other carriers and equipment manufacturers. In addition, this act establishes provisions for the use of information received from other carriers, as well as the ability of the carrier's agents to access customer information. The law's implications in the cyberworld would tend to protect the information of a user more securely than previous bills had. Unfortunately, this law also grants carriers the ability to use telemarketing advertisements.

The most recent and arguably controversial law passed is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. This act was a response to the terrorist actions committed against the United States on September 11, 2001. As the nation grieved for the victims in the airplane hijackings and crashes, this bill, which was initiated in the House of Representatives, was quickly created, amended, and signed into law within a record five weeks, with only one dissent. The 345-page bill makes changes

to over 15 different statutes as well as providing analysis and explanation to sections of the bill relating to new technological developments and online communications and activities. (Electronic Frontier Foundation 2001, 1)

The bill includes a plethora of information, such as some provisions that apply directly to combating terrorism, while other provisions seem to create and enhance laws governing the cyber-realm and regular non-terrorist activities. Such provisions include creating a counterterrorism fund, increasing funds to the FBI, expanding a national electronic crime task force, enhancing surveillance procedures, strengthening criminal laws against terrorism, and prosecuting international money laundering. Also mentioned are techniques on counteracting terrorist financing, protecting the national borders, establishing more stringent codes for immigration, removing "obstacles" in investigating terrorism, providing for the victims of terrorist attacks, and improving intelligence capabilities in both national and foreign spheres. (U.S. Public Law No. 107-56 2001.) Perhaps one of the most controversial aspects of the bill is that of information sharing between federal, state, and local law enforcement agencies, thus creating a centralized law enforcement and intelligence body. (U.S. Public Law No. 107-56 2001, Title VII: Sec. 701)

While law and immigration agencies have lauded the bill for unifying and increasing facilities in an abundance of fields, many critics, from the ACLU to online journalists and scholars, have attacked the bill for its confusing and intrusive language. Some critics, such as the Electronic Frontier Foundation, contend that Congress had failed to study the bill and that there was not sufficient time allotted to hear testimony from experts outside the law enforcement field where the changes will definitely be felt. In addition, critics

state that the government, which curbs some civil liberties in the law, failed to show that the reason they could not detect the planning of any terrorist acts stemmed from compromising previous laws and court judgments that established citizens' civil liberties. (Electronic Frontier Foundation 2001, 2) Moreover, this legislation increases the power of the president and executive branch subordinates; at the same time it reduces the power of congressional oversight in conducting domestic as well as foreign wars. (Herman, 2001 2) The problem which arises is Congress's refusal to maintain an active role in the oversight of the executive agencies. This weakens the federal check on the executive branch since the judiciary cannot make a decision until a controversy from this bill is brought forth to them.

Furthermore, in the surveillance provisions listed under Title II of the law, there is a decrease in judicial oversight of government surveillance, as well as a provision that allows a judicial magistrate to issue a court order for law enforcement officials pertaining to information outside his/ her district. (U.S. Public Law No. 107-56 2001, Title II: Sec. 215, Sec. 219) In essence, the surveillance provisions in the bill resemble the standards of the Foreign Intelligence Surveillance Act of 1978 (FISA). Title II, like FISA, allows for the increase in surveillance of activities, even when there is no probable cause. In addition, according to Title II, FISA warrants may now be used against citizens even if the purpose of the investigation is not to gather intelligence. (U.S. Public Law No. 107-56 2001, Title II: Sec. 225) This allows for the extension of nation-wide "roving wiretaps" to be used on intelligence wiretaps, which are secretly authorized and do not need

probable cause.[44] (Electronic Frontier Foundation 2001, 3) The possible privacy issue is whether or not a person being monitored, via electronic surveillance, will cause other users of that phone to be monitored. In addition, this law may restrict provisions created in the Katz and Alderman decisions, such as the two-pronged privacy test and the suppression of evidence against individuals whose rights were violated.

Advantages in this act to the average citizen and Netizen are few. Congress did place a sunset clause in Title II, section 224, of the provision, but this applies only to parts of the law. In Title II, only thirteen out of twenty-five provisions will expire on December 31, 2005. (U.S. Public Law No. 107-56 2001, Title II: Sec. 224) Those that will not expire include the continued sharing of grand jury information (section 203 a and c), the increased number of FISA judges (section 208), and the scope of subpoenas for records of electronic communications, which overrides the Cable Communications Act in respect to services offered by the providers (section 211). In addition, the modifications for "pen and trap" (section 216), single jurisdiction search warrants for terrorism (section 219), increased citizen assistance to law enforcement (section 222), and section 225 concerning FISA wiretap immunities will not expire.

The main problems of this bill are staggering. Not only is the law incredibly difficult to read for the average citizen, but one would need to go on a treasure hunt in order to comprehend the implications in the other laws that this act changes through amendments and edited provisions. Moreover, as some critics argue, it is obvious that close consideration of this bill was never taken. Section 217 of Title II of the bill contradicts

---

[44] Roving wiretaps are those wiretaps placed on all the phones that a specific person utilizes.

earlier amendments to the ECPA in section 203-(b) (6) (2) (B). In addition, it limits a person's due process rights under section 223 of Title II, and relieves the government of accountability through delayed warrants and amendments to the ECPA. There are actually so many criticisms of this bill that it is surprising that Congress and the President allowed it to pass with so many questionable passages and so little research.

Of course, as mentioned before, law enforcement and intelligence agencies have found this bill to be a boon to their previous information communication problems. The new law strengthens a new CIA-FBI alliance in two ways. First, the CIA is explicitly allowed to decide who will be targeted and the information to be retrieved on domestic investigations. In addition, the CIA is given full access to information on citizens that has been gathered by U.S. law enforcement agencies and grand juries. This might in turn allow the FBI to launch investigations into dissident groups or on an individual suspect whom they believe to have ties to terrorist or foreign intelligence agencies, no matter how remote the connection may be. (Dreyfuss 2002, 32)

Additional advantages may include the increased information local and state law enforcement agencies can now access through the FBI's Joint Terrorism Task Forces (JTTF). The JTTF and the USA PATRIOT ACT may help these local law enforcement agencies rebuild their intelligence units, so that they may have the ability to solve and tackle local terrorist problems. The only issue that the Justice Department fears is state and local agencies trampling the remaining privacy rights and civil liberties of groups and individuals who voice extreme political opinions. "Precisely because terrorism is a political crime, usually perpetrated by organizations with political agendas, antiterrorism intelligence can often mean surveillance of groups and individuals for their opinions and

not their acts." (Dreyfuss 2002, 33) As a result, the monitoring of political, racial, religious, and special interests, such as those concerning the environment, will be key factors in surveillance.

Through the development of legislation from 1934 until 2001, communications privacy has faced dramatic changes. Until the passage of the 2001 USA PATRIOT ACT, one could almost assume that privacy protections on the Internet were moving more in favor of personal privacy over that of government intrusion. Yet, with all violent actions, one must assume an extreme reaction to take place. Unfortunately Congress's reactions to the terrorist actions of September 11, 2001 have proven to be less favorable to Netizens' rights in cyberspace.

One hope to this outcome is that a case will present itself to the Supreme Court, and it will declare the unconstitutionality of this statute. While this seems unlikely, perhaps the ability to assert judicial power in the form of judicial review will tempt the justices to once again take a leading ethical role in the United States, as they did with Brown v. Board of Education. The other hope would be that Congress would see the error of this law and repeal it before it allows grave injustices not only to American society, but also to American Netizens. The last and most unlikely prospect will come from the American voters. Perhaps Americans will see the error in this legislation and make demands to rectify these privacy invasions by holding the government accountable, through either their congressional representatives or their president. If none of these actions come to pass, laws governing the cyberworld will not support the claims that some actions and communications in this realm are protected. As a result, Netizens may find the right to privacy a privilege allowed more so than an established prerogative.

CHAPTER IV

A NEW HOPE

Throughout this analysis, the clashes between the realm of electronic privacy rights and government's new crime solving applications have repeatedly turned up. The creation and use of programs such as DCS1000, Echelon, and encryption keys are just some methods that government can use to capture criminals. However, those same programs, when placed in the hands of an unchecked agency, can mean disaster to the constitutional rights of Americans. Shadows of McCarthyism and images reminiscent of those found in the movie "Gattica" and James Orwell's book Nineteen Eighty-Four creep into the minds of Americans. However, in the aftermath of the September 11th violence, many Americans who at one time defended their privacy rights now condone the government's intrusions, regardless of whether those intrusions protect them against harm in this integrated flesh and cyber-world. At the end of Chapter One, two questions that this analysis focused on were raised. They are: "Is there a protected constitutional right to privacy [in respect to the Internet]," and if so, "who or what will protect that right?"

In answer to the first question, the United States Supreme Court has said that the constitutional privacy rights of the individual do exist on many levels, including the new areas of communications. In addition, the Court stated that government could not intrude upon those privacy rights, even if the right is exercised in a public area. Government's

unwanted intrusion is a breach to one's right to privacy, and should not be condoned unless government can prove that there are sufficient reasons for encroaching upon the citizen's rights. Those reasons must be provocative enough to solicit a magistrate's concession to issue a court order such as in the investigation of suspicious or illegal activity or in the case of a national security breach. However, victims of privacy violations also have a burden to bear. Privacy does not encompass all aspects or realms of life. An individual must give up some autonomy when he or she enters into the social and political realm of society. The debate lies in where the realm of privacy ends and the realm of public information must begin. Those people seeking retribution for privacy invasions must be able to prove that their expected private communications with another individual took place in a location or realm that would be considered "reasonably private" in the eyes of society. (Katz v United States 389 U.S. 361 [1967])

For obvious reasons, the question of "reasonably private" areas versus not so private areas needed to be addressed. As discussed in the third chapter, Congress assumed the role of defining what privacy rights should be expected in different areas, especially in terms of abstract, technology-created areas due to new innovations in computer programming and mechanical engineering. Until the most recent USA PATRIOT ACT, Congress had upheld and attempted to clarify judicial decisions upholding the privacy rights of an individual in the technological or abstract world. However, since the enactment of the USA PATRIOT ACT, legislation upholding privacy rights has been weakened, if not dismantled.

As the courts and the legislature have maintained, there is a constitutional right to privacy in respect to the Internet. The problem that now exists is how much privacy is

protected on the Internet. As the end of Chapter Three suggests, this question can be answered only through the courts or the legislature. Until either branch deigns to answer this new dilemma, American Netizens can expect increasing problems and intrusions in their daily cyber-relations with other Netizens.

In answering the second question of, "who or what will protect this right to privacy," American citizens must look to a source other than themselves, since the U.S. courts have not established communication privacy as being a real constitutional right instead of an instituted statutory right. In the evolution of the Internet, it was discussed that the removal of government involvement caused a surge in cyber crime. U.S. privatized industry could not adequately regulate the transgressions that took place and invaded the personal privacy of American users. In fact, most users were not sophisticated enough in the protection of their own privacy rights, which helped produce the current problems that people face today in respect to cyber-stalking and identity theft. As a result, a cyber-governing agency and accompanying legislation must be created to protect the privacy rights infringed upon by the government (through use of the USA PATRIOT ACT) and cybercriminals.

Possible policy proposals for the creation of a new body and privacy protecting legislation would need to entail four premises that will allow the law to be dynamic enough that it may be interpreted to govern new innovations in technology over time. The new law would also need to be applicable to the privacy problems encountered in the cyber world. By the word applicable, it is meant that the law must be reasonable or must encompass possible problems that could arise. Fanciful propositions would only contribute to the edict's inability to mandate what would be considered legal and illegal.

Moreover, the laws and the governing body would not only have to apply to the United States, but also to an international audience, since the problems that are found on the Internet not only apply to the United States but also are ones that affect all countries that are linked to the Internet. Moreover, there needs to be a standard international law since each country's statutes, including the United States', has failed to establish adequate protection and institutions.

One of the first conditions that must be established in this possible new policy would be a universal provision that would be consented to by all countries, since one country's enforcement of laws will affect other Netizens around the globe. As it is, the current problem with many privacy laws involving the World Wide Web is that countries believe they can dictate their regulations to other countries' users. This can currently be seen in the Internet child pornography cases in Germany and the United Kingdom and their dilemma in relation to extradition problems involving users who send illicit child photographs from Singapore, which has loose child pornography laws. In addition, in respect to remailers, many times foreign anonymous remailers have refused to release users' identities to foreign countries. What this currently implies is that, if a hacker stalks an individual or releases a computer virus through e-mail, there is no guarantee that the hacker can be found and, if need be, extradited from a certain country. (Murphy 2001, 24-27)

However, if a universal agreement between all countries exists, cyber criminals may be held more accountable for their actions violating the privacy rights of individuals in other countries. The parties in a country that experienced the violation could address the suspect without having to negotiate through the bureaucratic mazes of the other

countries' extradition laws. Furthermore, as suggested in several European recommendations and supports, by sharing the experience of problems encountered over the Internet, the various national authorities can work together to adopt a coherent strategy for applying general principles on issues concerning data protection. (EU Directive 1998, 2.1.1)

In addition, in order to effectively enforce privacy protections and cyber law infringements, there must be a universally accepted governance body. A possible model could be the International Atomic Energy Agency (IAEA). However, unlike the IAEA, the proposed body would need the power to enforce legislation and pursue violators. The United States' Federal Trade Commission's Privacy Initiative Team also might be a potential model; however, like the IAEA, it too does not have the political clout, and in addition it lacks the initiative to take a firm stand on privacy policies, and so must also be ruled out. (Long 1997, 107) Possible sanctions on countries that accept the agreement, yet fail to implement local enforcement, could include trade sanctions and Internet boycotts of country originated sites. Perhaps even an extreme sanction might be an Internet blackout towards the country.[45] However, one big problem with international agencies is having adequate powers to enforce regulations and the accompanying violations. Consequently, many Netizens feel that private industry regulation and Netizen boycotts would be more effective. (Long 1997, 108) Yet as discussed, self-

[45] In terms of a "blackout" this could mean one of two things. Either the country's ISPs are temporarily shut down, or all sites originating from that country are displayed as negative and inactive. For example if the background is white, it becomes black or gray and the hypertext is neutralized.

regulation is ineffective in today's world, and thus a state supported agency must be created.

Secondly, while programs such as Echelon and DCS1000 will probably never be shut down, there must be another way to ensure the privacy of law abiding Netizens while at the same time pursuing illegal actions committed by cybercriminals. A possible proposal might be to secure a database with known "hacker" or cybercriminal trails. Unfortunately, anonymity, which goes hand in hand with privacy on the web, needs to be sacrificed when tracking known Internet-sophisticated computer felons so that other Netizens' privacy rights can be ensured.

Possible future implications might be stricter stipulations on the use of anonymous remailers and the purchase of encryption software. However, this provision would in no way require companies to give the new agency all access keys to their encryption software, nor would it provide that remailers furnish a complete list of users to the regulating body. Remailers could voluntarily offer a repeated offending user's name to the agency, should the remailers or private companies deem the transgression meriting punishment. An example of some transgressions could be a self-replicating virus or an e-bomb. Political speech, for example, would not be a punishable transgression but a protected right in the cyber world. In respect to encryption software, registering the purchaser at the time of purchase may be a possible option, but not a requirement. One main reason is that the purchaser could always acquire an encryption program somewhere without registering him or herself, such as over the black market. Remember, the premise of encryption software is to protect private communications and so access to those communications defeats the purpose of the program. As a result, Netizens' permission to

law enforcement accessing personal encrypted messages should be supported over legislation permitting access to encrypted information by law enforcement agencies.

In addition, there needs to be a universal standard of what information can be deemed "publicly accessible," or "public information." One of the problems Netizens face, as seen in the McVeigh case, is the easy access to personal information, such as gender and sexual preference. On some ISPs or BBSs, one's personal information might also include the last time a user logged on, his/her home address, phone number, and employer. These particulars need to be inaccessible to the average Netizen. In addition, one's credit information, medical history, and personal identification number or social security number also need to be made unavailable. All this "personal information" can be used to persecute a person, harass individuals, or perform fraudulent activities against that individual. Personal identity on the Internet must be protected by this agency since ISPs and the U.S. government have failed to do so. Moreover, there have been initiatives in the past that allow a user to "opt-out" or "opt-in" for advertisement requests as well as privacy controls. (Long 1997, 108) Unfortunately, these too do not have an impact on a user, who must become proactive and contact certain sites should they not want their information or "clickstream" to be sold or traded.[46]

Finally, the agency should perform random ISP checks on personal privacy. The philosophy behind random checks can be found in the retail world's "private shopper." The "private shopper" is an individual who inspects the quality of service provided in an average shopping experience. The experience usually begins once the shopper enters the

---

[46] A clickstream is a marketeering software tool used to track areas of cyberspace that consumers click to with a mouse. This information received may include what web sites were visited, the pages accessed, and the time spent on each page.

door of the facility, and ends after s/he completes a purchase and leaves the premises. The shopper then rates his/ her experience, and notes areas needing improvement, or areas/ actions that were neglected and/or violated the establishment's house rules. The belief is that, through random checks, services can be upgraded and maintained. This same philosophy can be applied to the ISPs. The premise is that random checks through an ISP on an isolated individual user will prove whether measures are taken to establish privacy controls allowing the distribution of minimal personal information. This may lead to a decline in the information trading market and identity theft. Services that a provider might offer could include the distribution of encryption software, identity certification or digital signatures, and stringent privacy regulation. The goal is to limit the public's accessibility to any specific user's information, thus limiting the possibility for a breach in security.

In the case of extradition or prosecuting cyberfelons and unlawful intrusive government agents, violators could be turned over to appropriate law enforcement agencies by the international body for violating international cyber regulations as well as country specific violations. There would be no differentiation between unlawful acts committed by a Netizen and unlawful acts committed by a government agent. There would be no requirement to extradite, but a country could request extradition if it wished. In addition, each country could include its accounts of crimes committed against that country by that individual or the government agency. The international agency would enumerate all offenses and provide a detailed list of all violations a suspect user committed. After being tried by a judicial committee for all crimes, the international

agency will issue a punishment for those offenses the criminal was found guilty of committing.[47] Perhaps this may seem like a naïve vision; however, the multistate-delegated power would establish the agency's global power in regulating and adjudicating Internet crimes. This agency could be the next step past a body like the United Nations, and could bring about whole new generation of effective international regulating bodies that supersede nation-state rules.

Conclusion

The Internet is a confusing and complicated world hidden beneath interactive commercial ads and "net" lingo. Unmanageable for the providers and seemingly unregulated, this virtual Wild West is slowly being tamed through governments' interventions. Yet, as government attempts to civilize this savage realm, it encroaches upon the privacy freedoms enjoyed by Netizens. American Netizens need to take a stand against government sanctioned intrusions committed against their privacy. United States courts have stated that there is a constitutional right to privacy for the communications and interactions in which Netizens partake. However, members of Congress are afraid to defend the right to privacy as a result of fears elicited from recent acts of violence.

The USA PATRIOT ACT is a disservice to the previous expanding cyber-privacy protections. This act needs to be reexamined by the Congress and the Supreme Court to either amend or repeal it. Its sanctions against criminal behavior cripple the electronic privacy rights that have just recently begun to make sense, and yet the act fails to apply

---

[47] This judicial panel might be compromised of the United Nations High Court, or it may entail judicial figures, chosen by each country governed by the cyber agency, which rotate every so many years.

strictly to terrorism, as some would purport it does. As a result of national agencies' overreactions to foreign and domestic violence, there is a need to create an unbiased international agency to protect the right of privacy that many western countries around the world profess to uphold. Without a regulating agency, there will be no body to sanction the transgressions that governments' law enforcement and intelligence agencies commit.

APPENDIX I

PRIVACY AMENDMENTS IN THE

U.S. CONSTITUTION

Amendment I
"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

In privacy rights, this Amendment is commonly used to refer to the aspect of freedom of speech and the freedom of association.

Amendment III
"No soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."

This amendment has been used in conjunction with the 4th Amendment to argue the rights of a citizen over that of the state, when it involves actions committed in one's own home.

Amendment IV
"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The 4th Amendment has been used to define the rights of citizens and the areas of protection for tangible and nontangible items. Some protected privacy zones are conversations, the right to read or view pornographic material, prophylactic rights between two consenting adults of different sexes, rights to contraception, the right to beget a child, and the termination of pregnancy.

Amendment V
"No person shall be held to answer for capital, or otherwise infamous crime, unless on presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor

shall be compelled in any criminal case to be witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

The 5th Amendment has been used to protect conversations and correspondence between two people as well as documents from a person, which would implicate him/her in a court of law.

Amendment IX

"The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

Often called the "catch all" amendment, the 9th Amendment has been used in conjunction with other amendments to protect privacy rights not specifically mentioned in the Constitution.

Amendment XIV, section 1

"All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

The 14th Amendment protects the right of due process for each citizen of the United States. This amendment has been used in the privacy realm of reproductive or contraceptive rights. In addition, it has been used in other arguments such the right to die. However, euthanasia has not yet been able to find a stable and favorable decision in the courts in protecting the right to terminate one's own life.

APPENDIX II

COURT CASES

Supreme Court

Alderman v. United States, 394 U. S. 165 (1968).
Boyd and other Claimants, etc., v. United States, 116 U. S. 616 (1886).
Griswold v. Connecticut, 381 U. S. 479 (1965).
Katz v. United States, 389 U. S. 347 (1967).
Nardone et al. v. United States, 302 U. S. 379 (1937).
Olmstead et al v. United States, 277 U. S. 438 (1928).
Stanley v. Georgia, 394 U. S. 557 (1968).

United States District Court

Timothy R. McVeigh v. William S. Cohen, et al., Civil Action 98-116, United States District Court for the District of Columbia (1998).

APPENDIX III

RELATED INTERNET WEBSITES

For information on Carnivore, check out the following sites:

- http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm
- http://www.msnbc.com/news/477749.asp
- http://www.epic.org/privacy/carnivore/foia_documents.html
- http://www.epic.org/privacy/carnivore/jud_comm.html
- http://www.epic.org/privacy/carnivore/kerr_letter.html
- http://www.epic.org/privacy/carnivore/army.html
- http://www.epic.org/privacy/carnivore/test_6_00.html
- http://www.epic.org/privacy/carnivore/projects.html
- http://www.epic.org/privacy/carnivore/deployments.html
- http://www.epic.org/privacy/carnivore/omnivoreproposal.html
- http://www.epic.org/privacy/carnivore/dragonnetproposal.html
- http://www.epic.org/privacy/carnivore/carnivorenotes.html
- http://www.epic.org/privacy/carnivore/carnivorequestions.html
- http://www.epic.org/privacy/carnivore/evolution.html
- http://www.epic.org/privacy/carnivore/phipletroenix.html
- http://www.epic.org/privacy/carnivore/purpose.html
- http://www.epic.org/privacy/carnivore/review1.html
- http://www.epic.org/privacy/carnivore/test1.html
- http://www.epic.org/privacy/carnivore.html

BIBLIOGRAPHY

Ahles, Andrea. 2000 "Surfers who Provide Personal Information to Site may be Surprised to Find Out How it's [sic] used" Fort Worth Star- Telegram (TX) March 29

Alexander, Cynthia J. and Leslie A. Pal. ed. 1998 Digital Democracy: Policy and Politics in the Wired World. Oxford, UK: Oxford University Press.

Anschütz, Dirk. 2001. "The Talk of the Web" On Magazine 6, no. 10:42-44

Associated Press. 2001. "Attacks renew encryption debate" MSNBC News: Invasion of Privacy. <http://www.msnbc.com/news/632280.asp> (20 November 2001)

Associated Press. 2001. "Judges protest computer monitoring: Group claims the practice is illegal" MSNBC Technology: Online Privacy. <http://www.msnbc.com/news/611195.asp> (November 20, 2001)

Balint, Kathryn. 1999. "Legislators debate Need for Internet Privacy Laws: Industry Representatives Defend Self- Regulation" San Diego Union- Tribune (CA) December 16

Barrett, Neil. 1996 The State of Cybernation. London: Kogan Page Limited

Bennett, Colin J. and Rebecca Grant. Ed. 1999. Visions of Privacy: Policy choices for the Digital Age. Toronto, Canada: University of Toronto Press

Bick, Jonathan. 2000. 101 Things you need to know about Internet Law. New York: Three Rivers Press

Biskupic, Joan and Elder Witt. 1997 Guide to the U.S. Supreme Court Third Edition. Washington, D.C.: Congressional Quarterly

Blank, Robert and Janna C. Merrick. 1995 Human Reproduction, Emerging Technologies, and Conflicting Rights. Washington D.C.: Congressional Quarterly Inc

Buderi, Robert. 1999. "The Virus Wars" Atlantic Monthly. 283, no. 4:32-37

Burstein, Daniel and David Kline. 1995 Road Warriors: Dreams and Nightmares Along the Information Highway. New York: Dutton Book

Canfield, Clarke. 1999. "Web Rule of Thumb: Logging on Means Signing off on Privacy." Maine Sunday Telegram (ME) December 26

Cate, Fred H. 1997. Privacy in the Information Age. Washington D.C.: Brookings Institution Press

Center for Democracy and Technology. 2002. "An Overview of the Communications Decency Act" Free Speech Online <http://www.cdt.org/speech/cda.html> (February 21, 2002)

Center for Democracy and Technology. 2002. "The Privacy Protection Act." Confidential Sources: Privacy Protection <http://www.rcfp.org/csi/ppa.html> (March 19, 2002)

Cohen, Adam 2001. "KEEPING AN EYE ON THINGS," On Magazine 6, no. 10: 48-56

Committee on the Internet in Evolving Information Infrastructure. 2001 The Internet's Coming of Age Washington D.C.: National Academy Press

Consumer Privacy Guide. 2001. "Privacy Protection Act of 1980" Protection Under Law <http://www.consumerprivacyguide.org/law/ppa.shtml> (March 19, 2002)

Coyle, Karen. 1997. Coyle's Information Highway Handbook: A Practical File on the New Information Order Chicago: American Library Association

Dam, Kenneth W. and Herbert S. Lin, ed. 1996. Cryptography's role in securing the Information Society. Washington, D.C.: National Academy Press.

Dawson, Ed and Jovan Golic, ed. 1996 Cryptography: Policy and Algorithms. New York: Springer

DeCew, Judith Wagner. 1997. In Pursuit of Privacy: Laws, Ethics, and the Rise of Technology. Ithaca, NY: Cornell University Press

Diffie, Whitfield and Susan Landau. 1998. Privacy on the Line: The Politics of Wiretapping and Encryption. Cambridge: MIT Press

Drake, William J. 1995 The Information Infrastructure: Strategies for U.S. Policy New York: Twentieth Century Fund Press

Dreyfuss, Robert 2002. "Spying on Ourselves: Bush's homeland- security team is building a massive surveillance state. Are we feeling safer yet?" Rolling Stone no. 892: 31-79

Drucker, Peter. 1999. "Beyond the Information Revolution." The Atlantic Monthly. 284 no. 4:47-57

Dube, Jonathan. 2001. "Growing Threat to Privacy World Wide: But countries recognize that privacy is a fundamental right." MSNBC Technology: Online Privacy. <http://www.msnbc.com/news/464096.asp> (November 20, 2001)

Electronic Frontier Foundation, comp. 2001 "EFF Analysis of the Provisions of the USA PATRIOT Act: That Relate to Inline Activities (Oct 31, 2001)" Electronic Frontier Foundation: Privacy: Analysis. <http://www.eff.org/Privacy/Surveillance/Terrorismmilitias/20011031-_eff_usa_patriot_analysis_of_the_provisions.html> (February 19, 2002)

Electronic Frontier Foundation, comp. 2001 "Marketing & E-Commerce Privacy" Electronic Frontier Foundation: Privacy: Marketing & Commercial. <http://www.eff.org/Privacy/Marketing.html> (February 19, 2002)

Ethical Spectacle, comp. 1996. "The Communications Act of 1934 was a Mistake." The Ethical Spectacle < http://www,spectacle.org/896/mistake.html> (February 21, 2002)

Etzioni, Amitai. 1992. "Teledemocracy: Ross Perot left the residue of a good idea behind him: the electronic town meeting" The Atlantic Monthly 270 no. 4: 34-39

EU Directive. E. C. 1999 Recommendation on the Respect of Privacy in the Context of Interception of Telecommunications.

Garfinkel, Simson. 2000 Database Nation: The Death of Privacy in the 21st Century. Sebastopol, CA: O'Reilly & Associates

Glanz, William. 1999. "Congress taking Slow Approach on Internet Privacy." Washington Times (DC) July 8

Gottfried, Ted. 1994 Privacy: Individual Right v. Social Needs. Brookfield, CT.: Millbrook Press

Grossman, Wendy M. 2001 From Anarchy to Power: The Net Comes of Age. New York: New York University Press

Gurak, Laura J. 1997 Persuasion and Privacy in Cyberspace. New Haven: Yale University Press

Guthrey, Molly. 1998. "New Privacy Right may Bring More Lawsuits: Impact of Supreme Courts Historic Decision Still Unclear" Saint Paul Pioneer Press (MN) August 17

Hall, Kermit L. 1992 The Oxford Companion to the Supreme Court of the United States. New York: Oxford University Press

Harper, Christopher. 1998. And That's the Way It Will Be. New York: New York University Press

Henderson, Harry. 1999. Privacy in the Information Age New York: Facts on File, Inc.

Herman, Susan. 2001. "The USA PATRIOT ACT and the US Department of Justice: Losing Our Balances?" The Jurist: Legal News Forum <http://www.jurist.law.pitt.edu/forum/forumnew40.htm> (March 17, 2002)

Howe, Walt. 1998. The Internet. Ed. Gray Young, New York: H. W. Wilson Company

Imparato, Nicholas, ed. Public Policy and the Internet: Privacy, Taxes, and Contract. Stanford, California: Hoover Institution Press

Jennings, Charles and Lori Fena. 2000 The Hundredth Window: Protecting your privacy and Security in the Age of the Internet. New York: Free Press

Kanaley, Reid. 2000. "Privacy Experts Say Internet Policies Are Not Reassuring" Philadelphia Inquirer September 28

Kommers, Donald P. and John E. Finn. 1998 American Constitutional Law: Essays, Cases, and Comparative Notes. Belmont, CA: Wadsworth Publishing

Kornblut, Anne E. 2000. "Cyberprivacy Catches Eye of Congress Bills Aim to Protect Consumers." Boston Globe (MA) June 19

Kunerth, Jeff. 1999. "You Have no Right to Privacy You Seek in our Open Society, Most Personal Information is Public, and it's Getting Even Easier to Find with High-tech Snooping." Orlando Sentinel (FL) August 8

Kutais, B.G. 1999. Internet Policies & Issues Commack, New York: Nova Science Publishers, Inc.

Langford, Duncan, ed. 2000 Internet Ethics. New York: St. Martin's Press

Laver, Murray. 1989 Information Technology: Agent of Change. New York: Cambridge University Press

Levine, Noah. 1996. "Establishing Legal Accountability for Anonymous Communication in Cyberspace" Columbia Law Review. 96, no. 6:1526-1572

Lipner, Seth E. and Stephen Kalman. 1989. Computer Law: Cases and Materials. Columbus: Merrill Publishing Co.

Liu, Melinda. 1999. "The Great Firewall of China." Newsweek.com. <http://newsweek.com/nw-srv/printed/int/wb/ov1315_1.htm> (October 6, 1999)

Loader, Brian D., ed. 1997. The Governance of Cyberspace New York: Routledge

Lockhart, William B, Yale Kamisar, Jesse H. Cooper and Steven Shiffrin. 1986. Constitutional Rights and Liberties: Cases- Comments-Questions. St. Paul: West Publishing Co.

Long, Robert E., ed. 1997 Rights to Privacy. New York: H.W. Wilson Company

Lyon, David and Elia Zureik. 1996. Computers, Surveillance, and Privacy. Minneapolis: University of Minnesota Press

Massingill, Teena. 1999. "Privacy Lost: Data Trail you leave is up for grabs." Contra Costa Times (CA) August 29

Mandell, Steven L. 1984. Computer, Data Processing and the Law. St. Paul, Minnesota: West Publishing Co.

Matias, Katie P. 2001. "THE TALK OF THE WEB," On Magazine 6, no. 10: 42-44

Meadows, Jack. Ed. 1991 Information Technology and the Individual. London: Pinter Publishers

Meeks, Brock N. 2001. "FBI's Carnivore has Partners: Declassified documents reveal e-mail snoop program [sic] details" MSNBC: Technology: Online Privacy. <http://www.msnbc.com/news/477749.asp> (November 20, 2001)

Meeks, Brock N. 2001. "Most federal sites fail privacy: 97 percent don't meet FTC standards for commercial sites" MSNBC: Technology: Online Privacy. <http://www.msnbc.com/news/458591.asp> (November 20, 2001)

Meyer, Marilyn and Roberta Baber. 1997. Computers in Your Future. Indianapolis: Macmillan Publishing

Miller, Steven. 1996. Civilizing Cyberspace New York: Addison-Wesley Publishing Company

Murphy, Stephanie. 2000. "Inter'Net'ional Influences: The Emerging Role of Internet Politics within the European Union" Governance 3: 24-28

"No Place to Hide: Invasion of Privacy." 2001 Discovery Science Channel DSCIE Television, December 17, 2001

Ojeda-Zapata, Julio. 1999. "Privacy, Please: The Realization that a Web User Gives Away a Little Bit of Information with Each Click of the Mouse Prompts the Creation of Protective Remedies that Range from Cryptography and Online Cloaking to Cyber-Privacy Legislation." Saint Paul Pioneer Press (MN) April 12

Palme, Jacob. 1995 Electronic Mail. Norwood, MA: Artech House Inc.

Pinkerton, John M. 1990. Understanding Information Technology: Basic Terminology and Practice Chichester, West Sussex, England: Ellis Horwood Limited

Plant, Raymond, Frank Gregory and Alan Brier, ed. Information Technology: the Public Issues. New York: St. Martin's Press

Quade, Vicki. 1996. "Text, Spies and Cyberspace: How the New Information Age can Affect our Daily Lives" Human Rights. 18-21

Reuters 2001. "'Big Brother' watching in Britain: Number of roadside speed cameras to increase" MSNBC Technology: Online Privacy.
<http://www.msnbc.com/news/613287.asp> (November 20, 2001)

Reuters 2001. "Interest in face scanning grows: Makers of technology struggle to meet demand since attacks" MSNBC Technology: Online Privacy.
<http://www.msnbc.com/news/630735.asp> (November 20, 2001)

Rose, Lance. 1995. NetLaw: Your right in the Online World. Berkeley: Osborne McGraw-Hill

Rosenoer, Jonathan.1997. Cyberlaw: The Law of the Internet. New York: Springer

Rotenberg, Marc. 1999. The Privacy Sourcebook 1999: United States Law, International Law, and Recent Developments. Washington D.C.: Epic Publications

Rubin, Michael R. 1988 Private Rights, Public Wrongs. Norwood, New Jersey: Ablex Publishing Corp.

Rubinstein, Geoffrey, comp. 1999. "Electronic Communications Privacy Act." Jones Telecommunications & Multimedia Encyclopedia
<http://www.digitalcentury.com/encyclo/update/ecpa.html> (March 19, 2002)

Schwartz, Evan. 1995. "Looking for Community on the Internet." National Civic Review 84 no. 1: 37-40

Schwartz, John and Robert O' Harrow. 1998. "Databases Start to Fuel Consumer Ire." Washington Post (DC) March 10

Scott, Gina Graham. 1995. Mind your own Business: The Battle for Personal Privacy. New York: Plenum Press

Smedinghoff, Thomas J., ed. 1996 Online Law. Reading, Massachusetts: Addison-Wesley Developers Press

Smith, Robert Ellis. 2000 Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet. Providence: Privacy Journal

Smith, Robert Ellis. 2000. Compilation of State & Federal Privacy Laws 1997: with 2000 Supplement included. Providence: Privacy Journal

Strum, Philippa. 1998. Privacy: The Debate in the United States since 1945 Orlando: Harcourt Brace & Company

Stuller, Jay. 2000 "Is Privacy Dead?" The American Legion Magazine 148 no. 5: 20-23

Sullivan, Bob. 2001. "They Know where you're shopping" MSNBC: Technology: Online Privacy. <http://www.msnbc.com/news/441058.asp> (November 20, 2001)

Swanson, Judith A. 1992. The Public and the Private in Aristotle's Political Philosophy. Cornell University Press, New York

U.S. Public Law No. 416. 73rd Cong., 1934. Communications Act of 1934.

U.S. Public Law No. 93-579 93rd Cong., 1974. Privacy Act of 1974

U.S. Public Law No. 96-440 97th Cong., 1980. Privacy Protection Act of 1980

U.S. Public Law No. 98-549 98th Cong., 1984. Cable Communications Policy Act of 1984

U.S. Public Law No. 99-508 99th Cong., 1986. Electronic Communications Privacy Act of 1986

U.S. Public Law No. 104-104 104th Cong., 1996. Telecommunications Act of 1996

U.S. Public Law No. 107-56 107th Cong., 2001. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001

Warren, Jay, Jay Thorwaldson and Bruce Koball, ed. 1991. Computers, Freedom & Privacy Los Alamitos, California: IEEE Computer Society Press

Warren Samuel D. and Louis D. Brandeis. 1890 "The Right to Privacy" Harvard Law Review: IV no. 5: 193-220

Westen, Tracy. 1998. "Can Technology Save Democracy?" National Civic Review 87 no. 1: 47-56

Wilson, Mark I. and Kenneth E. Corey. 2000. Information Tectonics: Space, Place and Technology in an Electronic Age. Chichester, West Sussex, England: John Wiley & Sons Ltd.

Young, Gray. Ed. 1998. The Internet. H.W. New York: Wilson Company.

VITA

Graduate College
University of Nevada, Las Vegas

Stephanie Ann Murphy

Home Address:
1252 Clifton Park Court
Las Vegas, NV 89110

Degrees:
Bachelor of Arts, Political Science, 1997
University of Nevada, Las Vegas

Publications

"Are We Cyber-Silenced?" Governance: The UNLV Political Science Review. 2:28-33 Fall 1999

"Inter'Net'ional Influences: The Emerging Role of Internet Politics within the European Union" Governance: The UNLV Political Science Review. 3:24-28 Fall 2000/ Spring 2001

Thesis title: WWW.PRIVACY.GOV: A Constitutional and Legislative Review

Thesis Examination Committee:
Chairperson, Dr. Michael Bowers, Ph.D.
Committee Member, Dr. Ted Jelen, Ph.D.
Committee Member, Dr. Alan Zundel, Ph. D.
Graduate Faculty Representative, Dr. Gary Larson, Ph. D.