Cyber-surveillance: A Case Study in Policy and Development

by

Richard S.Y. Kim

A dissertation submitted to the Graduate Faculty in Criminal Justice in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York

2010

This manuscript has been read and accepted for the Graduate Faculty in Criminal Justice in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy

_____	_____
Date	F. Warren Benton, Ph.D. Chair of Examining Committee
_____	_____
Date	Karen Terry, Ph.D. Executive Officer

Supervision Committee

_____
John Kleinig, Ph.D.

_____
Adina Schwartz, Ph.D.

City University of New York

ABSTRACT

Cyber-surveillance: A Case Study in Policy and Development

by

Richard S.Y. Kim
Advisor: F. Warren Benton, Ph.D.

The dissertation examines the historical development of surveillance, electronic surveillance, and cyber-surveillance from colonial times in the United States to the present.

It presents the surveillance laws, technologies and policies as a balance between national security and privacy.

To examine more recent developments, the dissertation includes case-studies of three cyber-surveillance tools: Carnivore, Magic Lantern, and NARUS; describing the operational functions, logistics, and search functions, and minimization capacities of these tools.

The closing chapters assess the dynamic balance between the achievement of national security and public order and the need to preserve rights and expectations of personal privacy.

Acknowledgements

This dissertation, which reflects my commitment to doctoral studies in Criminal Justice, is dedicated to Mother and Father, Bok Yun and Steve Kim, Dr. Ned Benton, Dr. Barry Latzer, Dean James P. Levine, Christina Czechowicz, Dr. Adina Schwartz, Dr. John Kleinig and Dr. Mary Gibson, and especially Grace, Julie, Sang-hyub, Michelle, Anna, and the Ramakrashna family for their unwavering support and grace, and Roger Deakins, and John Maynard, Nicholas Birsns, Lucy and Thomas Tucker, Kazmierz Kowalski and Dr. Adolf Soto.

I would like to thank Dr. Charles Lieberman, Prof. Daniel Boggiano, David Chenard, Instructor, New York City Police Academy, and Kathy Greene, and Jason W., Benjamin X. Liu, Dr. Patricia Miller, and Dr. Michele Lowrie.

I am most grateful to the CUNY Graduate Center and John Jay College of Criminal Justice for their generous aid and funding, and grants.

I would like to thank John R. and Jay K. and Rhoda Fisher for their friendship, and good cheer as I wrote my dissertation.

Table of Contents

Chapter One

Introduction: Surveillance, Technology, Law and Monitoring

The goal of this dissertation is to examine the history, law and policy of surveillance and cyber-surveillance in the United States from the origin of the nation to the present time, and to assess their impact on society and government. Surveillance has always been a tool of governance in times of national emergency. Police actions that intrude on privacy evolved into modern wire and electronic surveillance. After the World Trade Center attack, one must ask Juvenal's question: "Quis custodiet ipsos custodies?" to challenge the use of governmental surveillance authority, considering the consequences for personal privacy of changes in legal and operational criminal procedure, as well as technological capabilities for surveillance.

The dissertation also examines the conceptual, legal, policy and philosophical goals of the relationship between privacy, liberty and security. Can there be *stasis* (in contrast to a "balance"), where there must be a clear and present danger to warrant a trade-off of privacy for public security?

The dissertation explores the complex dynamics in the equilibrium between privacy, liberty and security, including those involved in governmentally mapping out the terrains covered by the presidency, courts, legislatures, and national intelligence and police agencies. Intelligence gathering and the investigative operations of Federal Agencies, as well as their monitoring should conform to constitutional rules, protections and measures.

Westin (1967:7) sets out a general definition that "Privacy is the claim of individuals, groups, or institution to determine for themselves, when how, and to what extent information about others is communicated to others." Modes of surveillance have expanded with the

evolution of high technology, so that privacy and the right to privacy are threatened in the 21st century.

DeCew (1997: 164) defines privacy in the technological era of our times in the following terms: "Privacy broadly categorized as a complex of three related clusters concerning information, access, and activities, is valuable because it shields us from interference, and threats of intrusion, scrutiny, ridicule, pressure to conform, and the losses that may bring access to one's physical person, or attempt to restrict behavior…..More self-regulation, systems of dynamic, and new legislative guidelines can prevent what often appears to be inevitable erosion of privacy."

Importantly, the major root of the problem is that surveillance justification, in periods of national crises, has always been part of the American experience. Constitutional and legislative norms order and regulate, and ensure a system of agency and judicial monitoring in light of the expansive growth of cyber-surveillance and surveillance technology. There are regulatory monitoring structures and the 4th Amendment that are intended to constrain intrusions on privacy.

However, the evolution of cyber-surveillance technology causes problems in the interpretation of the 4th Amendment law and Federal Statutory Law. Remedies should be provided to determine whether there is a breach of the law. The central problem is that the technology of the Internet, and network of cyber-surveillance systems is ahead of how the law can interpret and decide cases involving investigative and intelligence operations in the period following the World Trade Center attack. New initiatives for protection of privacy through legislation should assure that essential freedoms are not diminished or negated.

Moreover, the 4th Amendment, Federal Statutory Law and related oversight structures affect how we define privacy (on a policy, societal and philosophical level) as intrinsic

significant and personal values and liberties in a democratic society in which we are free to be anonymous and autonomous, without being under the radar or watching eye of any curiosity, scrutiny, or surveillance, whether it be the government, workplace associates or officials, hackers or foes.

John Kleinig (2009: 211) explains privacy as a type of moral agency: "Distinctive of mature human beings is their capacity to make and ordinarily be inclined to make decisions about how to live their lives in relation to others, their making those decisions with reference to moral or normative considerations…."

No certainties exist as to how cyber-surveillance technology will fare for the better or worse. We have reached a level of global surveillance that without firm legislative laws, chaos may result due to violation of constitutional freedoms and liberties.

However, since privacy is a paramount concern, the other central question in this study is: what are the "limits" to privacy? Amitai Etzioni (1999: 45) estimates such calculations under the rubric of "Scope, Nature, Threat" and magnitude of threat to public safety. He writes: "Privacy cannot be extended where it undermines the common good: conversely duties set to maintain social order cannot be expanded to the point where they destroy privacy." (Etzioni, 1999:199). We are left with the proverbial "policy paradox." The more than perplexing question is how to precisely measure the level of the scope, nature, and magnitude of the threat, which involves random probabilities of risk analysis in case of a terrorist attack. This is the significant inherent crisis of national security vs. constitutional freedoms, liberties and privacy rights dilemma.

If we see that information technology and cyber-technology have almost become universal phenomena in major parts of the world, the danger is that cyber-surveillance tools which possess almost ubiquitous monitoring capacities may fall into the hands of wrongdoers,

such as hackers and terrorists. Thus, the need for privacy protection is of utmost concern as a forewarning to what may lie ahead in regard to the advancement of cyber-technology and jeopardizing conditions.

Overview

The dissertation reviews developments in cyber-surveillance, taking into account the historical developments of law and regulation (oversight) as they have been applied to surveillance. Old regulatory measures failed, and were met with new governmental responses to privacy concerns.

Each historical stage and technology is examined in the light of nine factors that structure the legal and regulatory balance between national security interests and privacy interests. The following are the nine factors for understanding the status of privacy.

- **Theory and Definition:** The first factor is the theory and definition of privacy in the period or context involved.
- **Location:** The second factor involves the location of intrusion, particularly the legality of the seizure and opening of the mail whether in the agency or at a home.
- **Intrusion:** The third factor is the degree of intrusion involved.
- **Information Acquired:** The fourth factor is the nature of the information acquired, including the distinction between address information and message content.
- **Consent:** The fifth factor is the nature and timing of consent prior to intrusion or seizure.
- **Notice:** The sixth factor involves whether legal processes affirmatively require notice of the intrusion, and the nature and timing of the notice required. .
- **Third Parties:** The seventh factor involves consequences for third parties involved (e.g. government, informants, etc.) in the investigation and search.

- **Investigational Purposes:** The eighth factor involves the purposes of surveillance that are authorized.
- **Remedies:** The ninth factor involves the consequences for violators of laws and regulations, and the remedies to mitigate violence. These can include evidence suppression, fines and/or penalties for the violation of the law by the government.

Each of these factors is considered in the assessment, for each historical period or technology, of the balance between national security interests and personal privacy interests.

To examine this dynamic, the essay first presents a general history of postal surveillance in colonial America until the present time, modern mail monitoring and profiling techniques, proceeding with 4th Amendment law and Federal Statutory Codes in regard to the privacy of mail.

The third chapter opens with a general history of the emergence of telegraphy and wiretapping in the 20th century. A map of the techniques of wiretapping is provided. Also examined are questions concerning the differences between investigative and intelligence operations. A history of the rise of surveillance via the wiretap in the 60's to the 80's is provided. Then the chapter provides a history of Title III, ECPA, and the beginnings of federal statutory oversight. This section will also point to the new amended Title III (Title I) of ECPA, and CALEA, and it's legal impact and response. The chapter will conclude with a section on the status of privacy of the nine factors listed above, but applied to wire and electronic interception.

The fourth chapter begins with a general history of cyber-surveillance in the 1990's to the present time. It shows both the developmental and technical dimensions of how cyber-surveillance emerged on the Federal Law Enforcement scene to combat crime and terrorism. The

Federal and administrative responses to cybercrime and terrorism following the World Trade Center attack are then examined. The chapter concludes with a typology of cybercrime.

The fifth to seventh chapters are case studies of cyber-surveillance tools: Carnivore, Magic Lantern, and NARUS. Chapter five provides a technical overview and description of Carnivore. It then proceeds with the history and development of its system, including the technical means for agency and judicial monitoring and its legal implications. The chapter concludes with the status of personal privacy applied to this cyber-surveillance tool.

The sixth chapter examines the cyber-surveillance tool-Magic Lantern. A technical description and overview is provided, along with the history and development of the tool. A discussion of the technical means for agency and judicial oversight is provided, including an assessment of its legal implications. The chapter concludes with an assessment of the nine-factor status of personal privacy.

The seventh chapter is a case study of NARUS which is a tool for real-time intelligence monitoring for large-scale networks. The chapter begins with a technical description and overview of the tool. It then proceeds with the history and development of the tool, and the technical means for agency and judicial monitoring of legal compliance. The chapter concludes with the status of personal privacy applied to this cyber-surveillance tool.

The eighth chapter reviews, over the historical period of the study, the evolution of surveillance, and the consequences of that evolution for the status of personal privacy. The nine-factor framework is applied, triangulated with analysis and findings related to law, technology and procedure. This triangulation is the ultimate methodological attribute of strong case studies. (Yin, 2007).

The final chapter assesses the status of personal privacy in light of the entire scope of surveillance, from the inspection of mail through the most advanced technologies of cyber-surveillance, seeking lessons learned from history. The dissertation provides a cautionary historical narrative about the consequences of evolving technologies, and the need for vigilant protection of personal privacy by society when cyber-surveillance is in the hands of criminals, hackers, and government agencies.

Chapter Two

Postal Surveillance During the American Colonial Period Until the 20th Century

2.1. Postal Surveillance During the American Colonial Period

The original establishment of the United States Postal Service is connected to the British Government and its Postal System, established by William III in 1691. It was not until his Majesty's Postal System dismissed Benjamin Franklin, who as Deputy Postmaster General was countering the interception and opening of mails that advocated American Unionist Government, that the Continental Congress pressed forward to establish an American Postal System arranged through states, regional townships, and principalities in the advent of the American Revolutionary War. The Continental Congress declared (Fowler, 1977: 3): "The present critical situation of colonies renders it highly necessary that ways and means should be devised for the speedy conveyance of intelligence from one end of the Continent to the other."

Between 1774 and 1775, in the context of the Battles of Lexington, Concord and Fort Ticonderoga, the Continental Congress advocated a separation from the British Postal System to uncompromisingly secure the intelligence and patriotic letters of the supporters of the American Unionist Government. In July 26, 1775 the American Postal System was established. One purpose of the establishment of the American Postal System was to fully secure the accountability of critical intelligence information and data which were being compromised and tampered with by the British Postal System, to safeguard patriotic Americans, who supported independence from Britain, in light of the events which led to the American Revolutionary War. The American Postal System, with the Post Master General who was a member of the President's Cabinet, was established to counter-act and free itself from the surveillance of the British Postal System through its parcel carrying, which had controlled and regulated political

freedoms through the interruption, tampering and destruction of the anti-British intelligence and communication carried through the postal system.

However, the use of surveillance in the American Postal System includes many controversies throughout its political and social history involving censorship, suppression of "incendiary materials, subversive activity and acts of treason against the U.S. government." Incendiary material[s] in 19th Century America which were routinely suppressed involved publications pertaining to state secession, Civil War, slavery and the Abolitionist Movement, and "obscene mater, lascivious, faith and morals corrupting materials," and financial fraud connected to bogus lotteries, and advertisements in newspapers, and device and objects used to obstruct or destroy the U.S. Postal Mail System.

These forms of mail were, according to Fowler (1977), "unmailable," and prosecuted by law. This roughly constituted the Postal Code from the mid to the late 19th Century. Fowler seems to suggest that such materials were not so much surveilled but searched from the parcel, mailing imprinting and engravings on the mail. However, the postal inspectors were not authorized to open the mail.

From early to mid-20th Century, there were highly volatile issues in which surveillance and subsequent censorship and confiscation of "subversive, un-American mail" were treated as political sedition to overthrow the American government as to incite violence. In 1917, Congress (Fowler, 1977: 111) had enacted a bill to exclude mail that was in nature "anarchistic and treasonous" and "of a character advocating the destruction or injury to Government with violence." This bill had passed by more than a majority house vote in Congress. During 1913-1921, the Postmaster General implemented provisions of Title XII of the Espionage Act of June

15, 1917. Procedural rules were created that would exclude illegal publication from any mail under the Espionage Act (Fowler, 1977: 113) and Trading with the Enemy Act.

The Postmaster General, who was responsible for carrying out the provisions of the Espionage Act, such as censoring, detecting, and surveilling mail, during the WWI and WWII, grew strong through the turbulent period during the five wars the U.S. fought in the past century. No trade or commerce was permissible with a group or enemy that opposed the U.S. government via mail. The enforcement of the Espionage Act consisted of censoring, excluding, and surveilling the mail of communists, anarchists, and other subversive groups, then known as the "third-pillar." However, domestic letters could not be opened unless pursuant to a special Federal search warrant. Individuals or social and political groups who were considered subversive or considered to be aiding foreign powers, or those who were involved in organized crime, were surveilled through the postal inspection system.

2.2 Modern Mail Monitoring and Surveillance

The surveillance procedures of the USPIS are intended to ensure that they defer to the "sanctity of mail." The procedure is maintained through what is known as their "Mail Cover Process." The mail cover is a process in which a non-consensual record is made of any data appearing on the outside of mail. This step allows law enforcement authorities to copy the "To and From" (front and back side) of the envelope, without either the sender or the recipient's knowledge.

The mail coverage process is under the authority of the Chief Postal Inspector. A postal inspector makes a request for a mail cover assuming that the mail cover will produce evidence relating to violation of the postal statute.

- A postal inspector's request is under the authority of the Chief Postal Inspector.
- Where requested by law enforcement agency where reasonable grounds are laid out to as necessity.

The mail cover has been upheld, in one case concerning the fourth amendment, in the *United States vs. Choate*, 576 F. 2nd 165. In this particular case, the court determined that recording the mail cover did not violate the right to privacy, freedom of speech or freedom against unreasonable search and seizure because the mail was not opened. Moreover, in such a case, there is no reasonable expectation of privacy regarding the outside of the envelope.

2.2.1. Search Warrants for Mail

First Class mail and parcels are protected against search and seizure under the Fourth Amendment, and thus cannot be opened without a search warrant. This applies to mail which originates in the U.S. Significantly, the restrictions on mail over must not pass the threshold requirements of the sanctity of the seals of mails with probable cause and a warrant.

2.2.2. Codes of Federal Rules of USPIS: Authority of Postal Investigation

The primary focus on postal investigation can be illustrated in 39 Code of Federal Regulation 2331.1 *Arrest and Investigative Powers of the Postal Inspectors.* As for the authorization process, postal inspectors can serve warrants and subpoenas to make arrests without warrants. The USPIS has the power to make arrests without warrants for felonies cognizable under the law of the U.S. if it has reasonable grounds to believe that the person has committed a crime, or is about to commit a felony. USPIS also has the power to seize property under the authority of the law. In addition, "to the extent that is authorized by the Attorney General pursuant to agreement between Attorney General and the Postal Service, if the

enforcement of other laws of the United States … if the Attorney General determines the violation of such laws will have a detrimental effect upon the operations of the Postal Service."

The most important point in postal surveillance is that the Postal Inspector or Officer must deliver the illicit mail, and a search warrant is to be declared legal and authorized to ascertain that a felony has been committed.

2.2.3. Profiling Technique in Postal Surveillance

In 1998, U.S. Postal Surveillance Inspectors proposed a new partnership with the Omaha, Nebraska Police Department (Langan and Vajgert, 1996). With a high volume of narcotic arrests, considerable amounts of illegal substances were distributed through the mail. Postal Inspectors and the Omaha Police tracked down gun-running and drug trafficking from Southern California to various regions including Omaha.

"Analytic profiling" techniques were used to isolate and restrict suspicious looking packages based on labeling, and based on where the postage was to be placed and sent. This involved scrutinizing "labels" and "emblems" from sender and addressee parcel posting.

Package labels and emblems were investigated as clues to the suspicious identities of the criminal offenders, in terms of packages containing contraband, masking tape, addresses, and names, and the addresses of the location to where the packages were sent. This step anticipates where these suspicious packages were being sent to, in lieu of mail covers, and search warrants. And then with a dog sniffing crew, the packages were traced to sender and addressee, whereupon arrests were made.

The significance of such a postal surveillance analytic technique was that this implemented a "reconnaissance systems approach" to track illicit mail and parcels based on their

packaging and addressing, followed by careful step-by-step coordination with patrol and postal investigative leads. The new process worked well.

The investigative authority of the Postal Inspection Services partnered with local law enforcement in adherence to FCR, and the mail cover process, and constitutional rules of search and seizure can be seen as a success in observing privacy, and the sanctity of mail, with added measures of analytic profiling techniques.

2.3. The Status of Personal Privacy

The status of personal privacy in this period is reinforced by a general application of the rule of the sanctity of mail seals, unless posed as a threat to national security. The sanctity of mail seals cannot be revoked unless there is a threat to national security, or investigation to crime.

It is in the codified policy of the U.S Parcel Service, then and now, that "privacy and security of mail under a long standing frame under Federal and Statutory Regulations strictly safeguard, i.e., the envelopes, wrappers, as well as contents and all information ... which includes all information about the incipient that is contained in the mail-piece. The Postal service does not collect or store information that would allow the Postal Service to identify the record except with these strict statutes and federal regulations." (U.S. Parcel Service, 2008). This policy is known "Intelligent Mail Privacy."

The following is an assessment of the status of personal privacy during this period based on the nine-factor analysis set out in the first chapter of this essay.

2.3.1. Theory and Definition

During this period, the core theory of privacy protection involved the sanctity of mail seals, and the distinction between the mail cover and the content of the letter or package.

Under the Fourth Amendment, people are protected from the opening of sealed mail absent a warrant supported by probable cause. *See, e.g., United States v. Jacobsen,* 466 U.S. 109, 114 (1984); *United States v. Van Leeuwen,* 397 U.S. 249 (1970); *Ex parte Jackson,* 96 U.S. 727, 733 (1877). In *United States v. Ramsey,* 431 U.S. 606 (1977), the United States Supreme Court held, however, that the border search exception to the warrant and probable cause requirements of the Fourth Amendment applies to incoming international mail. Under the border search exception, "searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border." *Ramsey,* 431 U.S. at 617. The Court further recognized that "the 'border search' exception is not based on the doctrine of 'exigent circumstances' at all. It is a longstanding, historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained." *Id.* at 621. Since the border search exception applied, the *Ramsey* Court held that the defendant's Fourth Amendment rights were not violated by the warrantless opening by a Customs Inspector of a sealed, bulky package that had arrived in Kennedy Airport from Thailand. The Court reasoned that the opening of the sealed package was justified because, as required by postal regulations, the inspector had had reasonable cause to believe that the package contained narcotics. The Court specifically noted that the postal regulation's "reasonable cause" requirement was less strict than the Fourth Amendment requirement of probable cause. The *Ramsey* Court further reasoned that no free speech issue was raised under the First Amendment because the "[a]pplicable postal regulations flatly prohibit, under all circumstances, the reading of correspondence absent a search warrant, 19 CFR s 145.3 (1976): No customs officer or employee shall read or authorize or allow any other person to read any correspondence contained in sealed letter mail of foreign

origin unless a search warrant has been obtained in advance from an appropriate judge or U.S. magistrate which authorizes such action." *Ramsey*, 431 U.S. at 623.

The USPIS granted more than 10,000 requests from law enforcement agencies to record the names and addresses on mail sent to Americans for criminal investigation, but wouldn't disclose the number of mails investigated for anti-terrorism investigations (**http://www.usatoday.com/news/nation/2008-03-05-mail_N.htm?loc=interstitialskip**). The same source cites, that in 2004, 2005, and 2006, officials granted 99.5% of the requests.

There is one exception to the rules in respect to sealed mail, which is postal mail in which addressee and envelope information that is voluntarily in plain view to third parties, and postal inspectors (see United States v. Choate, 576 F.2nd, 165 (9th Cir. 1978, United States v. Jacobsen, 466 U.S, 109, 114 (1984) and United States v. Leon Van Leewen, 397 U.S. 249 (1970); see also, United States v. Hernandez, 313 F. 3rd 1206 1209-10, (9th Cir. 2002). Although has a person has legitimate interest that a mail will not be opened and search en route, there can be no reasonable expectation that postal service employee that will not handle the exterior.

2.3.2. Location

During this period, location mattered because locations are specific: the origin and destination of the piece of mail, and the physical location of the piece of mail when in the custody of the postal service.

Although a warrant and probable cause is required for the opening of sealed, domestic mail, under the border search exception, these requirements do not apply to incoming international mail. As seen above in the discussion of *United States v. Ramsey*, 431 U.S. 606 (1977), postal regulations do, however, require officers to obtain a warrant before reading incoming international correspondence.

2.3.3. Intrusion

There is no physical intrusion, other than the investigative monitoring of the U.S. Postal Inspectors when they investigate postal crime with probable cause, and a search warrant under the 4th Amendment, when post and parcel is sealed. The only other alternative is the mail cover process and postal profiling as previously stated.

2.3.4. Information Acquired

USPIS inspects and investigates any violations of 39 C.F.R.233.33., and the knowledge thereof in respect to postal law. Title 19 S.C. 82 implements the postal regulations to intercept and retrieve incoming mail, when they have "reasonable cause to suspect" that the mail contains illegal content (although the regulations prohibit the reading of correspondence absent a search warrant.) This was the key alleged violation of the 4th Amendment law in regard to reasonable search without probable cause in *U.S. v. Ramsey*, 431 606 (1977).

2.3.5. Consent

During this period, consent was required before mail could be opened for inspection. According to Peter Rendina, National Public Information Officer (USPIS personal communications, 2008):

> "The law generally requires an expectation of privacy in the mail to grant consent to open. In most cases, the law only recognizes that expectation of privacy as being held by the sender or the addressee. Thus, third party consent will not be available in most cases prior to delivery of the mail."
>
> "Under ASM 274.21(b) Postal Inspectors can open mail with the consent of either the sender or the addressee."
>
> "Under DMM 507, the sender can 'recall' mail that he has placed into the mailstream before it has been delivered (we usually use a PS Form 1509, but it is not absolutely required). Once the mail is retrieved, the sender can then grant consent to open, retain, and dispose of the mail."

2.3.6. Notice

During this period, only with notice can contents (communications and parcels) be opened, including a warrant under 4th Amendment protections. Under the condition of the mail cover mail can be withheld from the addressee, and then delivered when under the authority of the USPIS in cognizance of violation of postal law (**http://law.justia.com/us/cfr/title39/39-1.0.1.4.21.0.1.3.html**). A mail cover is issued for reconnaissance for criminal investigation purposes.

2.3.7. Third Parties

During this period, third parties could not authorized with regard to the opening and inspection of mail. Peter Redina, National Information Officer of USPIS (personal communication, 2008) states:

"Commercial mail receiving agents and others to whom mail is addressed in care of, do not have an expectation of privacy, and, therefore, cannot consent to anyone opening it, even after delivery. This is different from UPS, FEDEX and other common carriers which specifically and contractually reserve the right to inspect the contents of items shipped with them."

2.3.8. Investigational Purposes

The investigational purposes and goals of monitoring and surveilling of mail are limited to criminal investigations, national security threats, and searching and seizing fugitive mail. Outside of warrant and 4th Amendment protections, the USPIS is limited to conducting searches and seizures of contents in post and parcel, other than what can be viewed from the exterior.

2.3.9. Legal Remedies

Under the exclusionary rule of *Weeks v. United States,* 232 U.S. 383 (1914), and *Mapp v. Ohio,* 367 U.S. 643 (1961), evidence obtained in violation of the Fourth Amendment is inadmissible in criminal prosecutions. The exclusionary rule has been subject, however, to

increasingly severe exceptions. *See, e.g., United States v. Leon*, 468 U.S. 897 (1984); *Hudson v. Michigan*, 547 U.S. 586 (2006); *Herring v. United States*, 129 S.Ct. 695 (2009).

Chapter Three

Telegraphy, Telephony and Wiretapping

3.1. General History of the Emergence and Development of Telegraphy and Wiretapping

The emergence of telegraphy in the U.S. was a 19th century development between 1833 and 1866 (Nonnenmacher, 2007). In 1832, Samuel Morse conceived a single wire device to transmit electromagnetic signals commonly known as "Morse Code." It was patented in 1838. He obtained a grant from Congress to build an experimental telegraph line from Baltimore to Washington DC. The invention of the telegraph was successful. Between 1866 and 1900, Western Union won monopolies in setting up the largest telegraph services and communication systems. The telegraph system was needed as a telecommunication information resource for the railway systems, the New York Stock Exchange, and other financial markets and trade.

During the Civil War, there were many telegraph companies that wired messages across the United States, and the number of companies involved reinforced privacy because intrusion would be complex. Another limit on intrusion, in contrast to the U.S. Postal System, was that companies like Western Union were private enterprises. It was not until the Civil War that the telegraphs were tapped. This was executed by the Confederate and the Union governments as military operations to intercept, confound, and destroy intelligence information of the opposing army.

There were many cases in which owners of telegraph companies refused to provide private telegraph messages because it violated their policies of maintaining privacy for all users. However, many telegraph companies succumbed to the pressures of the Congress that they must

reveal telegraph messages in order to win the Civil War. The private telegraph companies were subpoenaed to hand over the wired telegraphy copies.

The "tapping technologies" of the 19th Century became "wireless wire tapping technologies" of the telephonic system. The first police operation of the "wire tapping" involved the case of *Olmstead vs. United States,* 277 US 438 (1928). The police wiretapped the phone lines of Roy Olmstead, who was involved in the smuggling of bootlegged liquor. The wiretap was physically placed in the basement area of his home. The legal issue that resulted was whether a search warrant was necessary for a wiretap. The Court ruled the wiretap constitutional because it was not a physical invasion of Olmstead's property.

However, in *Nardone* (1937), according to Diffie and Landau (1998: 133), "the Supreme Court avoided constitutional questions and used the Federal Communication Act as a basis for making warrantless wiretapping illegal."

The history of wiretapping has various uses, among them (Difffie and Landau: 1998:151) the "installation and use of wiretaps by the police, intelligence agencies, honest citizens, business and criminals." This is akin to "eavesdropping" and "lettering opening," granted that such controversial activity may not cross the threshold of governmental illegality, where there are no procedural or oversight laws to warrant intrusion of privacy or illicit surveillance.

However, in *Katz v. United States,* 389 US, 347 (1967) the Court ruled that evidence obtained from a warrantless wiretap, placed in public phones, was inadmissible. Some scholars have claimed that with the landmark *Katz,* (Diffie and Landau 1998: 167) the Court "changed the U.S. wiretap law." They claimed that, unlike the *Nardone* decision, which relied on statutory interpretation, the *Katz* case is based on underlying principles of the Constitution. The Supreme

Court arrived at the views that bugs and wiretaps as a form of a search are permissible, but subject to the limitations and protections laid down in the Fourth Amendment (167).

There were two focal, "high points" in the early to the mid-late 20th Century in which the use of wiretaps were considered viable alternatives for two other methods. First, wiretaps were used to combat threats to domestic national security and organized crime which was considered a growing problem. Second, wiretaps were used to ensure regulatory laws and a oversight framework of Title III of the Telecommunication Act [1968] which provided the "search warrant" parameters and "minimization" guidelines of what constituted a use of wiretapping. Like the censorship and surveillance of mail by the Postmaster General for subversive activity, and threats to national and domestic security, wiretapping was used by law enforcement agencies and intelligence agencies to monitor wireless messages, which can be used to harm public safety and commit fraud through the political and social upheavals, conflicts and wars of this past century.

3.2. The Mechanics of Wiretap

According to Diffie and Landau (1998: 115), wiretaps are placed in the microphone of the handset, which may be connected to the phone by wire, or by radio in case of wireless phones. The wire communications are passed down from phone from a line cord to the wall socket. If the phone is in an office building, the wiretap is connected to the closest phone of the phone that needs to be tapped. On the other hand, if the phone is in a private residence, the signal goes directly to a junction box on an outside wall, and then is wired to a pole. In this situation, the wire goes a short distance until it is routed underground. Then, at this point, the signal travels a far distance, and makes its way to a local phone exchange.

3.2.1. Uses of Wiretap in Law Enforcement: Purposes and Goals

In the modern era, with the advancement of telecommunication, one of the central elements in "hard cases" to obtain evidence for criminal prosecution involves the use of wiretaps to obtain information about illicit and criminal plans of offenders. This can be done primarily in two ways (Diffie and Landau, 1998: 113). The first way is through conversation between a criminal and an undercover police officer, and the second way is through conversation between criminals being overheard by police or agents.

Due to the wide scope of criminal planning or organizational activities, when the victims are unknown, the use of the second option of wiretapping to break or intercept the walls of communication of organized criminal activity has been a common way for police and law enforcement to prosecute offenders.

The use of wiretaps still remains to repress and investigate criminal networks engaged in conspiracy, and it has been the most consistent method in fighting organized crime, espionage, and high-tech crime involving drug traffickers.

3.2.2. Wiretapping and Investigative/Intelligence Operations

The most common forms of wiretapping in law enforcement are reactive and pro-active wiretapping. As Alberti (1999: 2) states: "The majority of investigations conducted by law enforcement are reactive; the investigation has already occurred. The facts of the have been established, the investigator must clarify and identify them." In contrasting with the "pro-active," Alberti further points out that in such cases criminal activity is very much ongoing and "yet not actually identified as one distinct incident." Importantly, as the operational basis of wiretapping techniques, the fundamental goals are as Alberti claims, "tactical" and "strategic."

"Tactical intelligence is short term, evolving into immediate active investigation with the objective of arrest and prosecution." (1999: 2)

Furthermore, Alberti (1999: 2) states: "Strategic intelligence consists of long term objectives and goals. Data are continually being collected and analyzed to reveal patterns of organized criminal activity. Strategic intelligence starts with raw data that are unsubstantiated, requiring investigation for confirmation, thus becoming hard data." Nonetheless, Alberti lastly points out that tactical and strategic intelligence, though different, overlap and work together as operational techniques.

3.3 Surveillance in the 1960's-1980's: Organized Crime and National Security

Wiretapping of intelligence-related information by intelligence agencies differed from wiretapping by law enforcement agencies. A law enforcement agency investigates and seeks evidence in criminal prosecution. Clearly, this is not the case for intelligence agencies which seek non-criminal informants and may also seek to confiscate, confound and destroy information.

In 1966 J. Edgar Hoover said: "La Costra Nostra is the largest organization of the criminal underworld in this country, very strictly disciplined." (Carrol, 1967). Robert F. Kennedy, who was then U.S. Attorney General, while counsel to the Select Senate Committee on Improper Activities in the Labor or Management Field, investigated labor racketeering and uncovered ties between the unions and organized crime. Congress soon passed legislation that Kennedy had requested to fight organized crime. The goal of the legislation was to break into the world of informational secrecy of subversive groups, criminals, and spies. Law enforcement and intelligence agencies, according to their strategic modes of operation, made the argument

that "wiretapping" is a necessary evil to combat groups, whose secret information presents risks of harm to the state.

3.4 Title III, ECPA and CALEA Surveillance as Federal Statutory Oversight

In the United States the instrumental use of wiretapping technologies was regulated and enforced by the Communication Act of 1934. This act was formed from parts of earlier legislation, and the interpretation of the Act is in accordance with Supreme Court's decision of *Olmstead v. United States,* and *Nardone v. United States*. (Barker, 2006:2). According to Barker: "These controversial and criticized decisions held that law enforcement were banned only from divulging the content of the communication that law enforcement could legally monitor communication without much regulation, and were banned from the divulging of the contents of the information, especially for the use of evidence."

It was not until the passage of the Omnibus Crime Control Act, commonly known as Title III, that a comprehensive set of rules was put in place to regulate wiretapping. As a result, the prevailing philosophy of the legislatures supported minimal safeguards to make electronic surveillance acceptable to combat serious crime as well as for the use of monitoring threats to national security.

3.4.1. Legal Response to Title III

There were several legal and judicial responses to Title III (1968) regarding the regulation of wiretaps. Congress disallowed the "most unregulated type of interception that been allowed for the previous forty years." (Barker, 2006:2). Intercept warrants were required and mandatory for surveillance operations. The further requirements must meet "strict conditions of necessity, minimization, and probable cause before a judge." This was a way the judge placed a check on unlawful investigation.

3.4.2. The Impact of ECPA and CALEA

According to Barker (2006:3), the modern regulation of electronic surveillance began with the Electronic Communication Privacy Act (ECPA) (1986) because of the impending use of technology. It amended Title III to respond to new technologies, by "replacement of aging legislation." A major problem which Barker points out is that ECPA pre-dated the great access to the World Wide Web, which was well before the creation of the Internet. The issue of how Title III's requirements would be met through the use of law enforcement's outdated electronic surveillance under Title III's regulation was a pressing issue for legislation in Congress.

3.4.3. Legal Response to ECPA and CALEA

As Barker points out, the most critical debate in the regulation of ECPA was to discern the differences between the substance of a communication (content) and its attributes.[1] In keeping with the vestiges of Title III requirements set to new technologies, ECPA requires a warrant for the interception and surveillance of the substance of the communication. It requires a subpoena or court order for the interception of a communication's attributes as done through a pen and trace. In light of such a development, ECPA can be considered an updated version of Title III.

The Communications Assistance for Law Enforcement Act was passed in 1986. The goal of this Act was to set a co-operative partnership with Law Enforcement agencies to assist them with wiretapping[2]. Due to the expansiveness of wireless technology, law enforcement agencies needed the help of telecommunication agencies with technology to combat serious crime and

[1] For example, such information as the number called, the identities of the parties subject to the call, the time and date of the call's placement.

[2] The distinctions made by ECPA include dividing communications up into categories for purposes of enforcement, including real-time acquisitions, information acquired out of short-term electronic storage, and information acquired out of long-term storage, and storage for backdrop protection. See Daniel Solove's analysis of these distinctions, "The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy and the USA PATRIOT ACT: Surveillance Law: Reshaping the Framework: Electronic Surveillance Law." 72 Geo. Wash. L. Rev. 1264, (2004). pp. 8-11, also, LaFave et al., (2004) pp. 231-234.

threats to national security. As Barker clearly points out (2006: 3) "The main thrust of the Act operates to assist law enforcement agencies in electronic surveillance, but only pursuant to a warrant or court order. CALEA accomplishes this goal by requiring telecommunications carriers to ensure that their equipments, facilities, or services are capable of allowing a lawfully authorized government agency to expeditiously isolate and intercept wire and electronic communication carried by the network, transmitting the intercepted communication to the government in a reasonable format."

3.5 Status of Personal Privacy

Berger v. New York, 388 U.S. 41 (1967) was decided one year before Title III, the Omnibus Crime Control and Safe Street Act (1968), 18 U.S.C. 2510-2520 was enacted, in which there was added 2701-2710, having to do with stored wired and electronic and transactional records access. Other significant cases were *Katz v. United States,* 389 U.S. 347 (1967), FISA Amendments Act (2008), and Restore Act (2008). These provided the general framework for the status of privacy analysis in telephonic surveillance. The two landmark cases and Title III, amended by ECPA (1986) regulate the legal mechanics and policies of how telephonic interception is defined and operationalized to ensure privacy protection. The FISA Amendments Act (2008), and Restore and Protect Act, which expanded the power of the state to wiretap in accord with national security interests.

Title III came about due to the egregious lack of procedure with regard to the hazards of police bugging described in *Berger v. New York,* (Lafave et al, 2004). There was too much expansive power by the police to wiretap without procedural safeguards. The following is an assessment of the state of personal privacy based on the nine-factor rubric set out earlier in this essay.

3.5.1. Theory and Definition

Post *Berger,* Congress enacted Title III to limit police power to telephonically wiretap by precisely defining the meaning of interception, judicial approval and oversight, and statutory procedural operations. Under Title III, police or certain subordinates may authorize application to a federal judge for a wiretapping. An interception order may be issued only if the judge determines, on the basis of facts submitted, that there is probable cause for belief that an individual is committing, or has committed, or is about to commit an enumerated offense. There must also be probable cause to believe that communications concerning that offense will be obtained through such interception: that normal investigation procedures have been tried or failed, or reasonably appear unlikely to succeed. (LaFave et al., 2004).
et al, 2004). The identity of the target must be specified, along with a particular description of the type of communication and of the person authorizing the application, to which it relates or the identity of the agency authorized to intercept the communications and of the person authorizing the applications, including a statement whether or not the interception is authorized, or including statements, whether or not he interception shall be automatically terminated.. (LaFave et al., 2004).

3.5.2 Location

Katz v. United States, 389,U.S. 347 (1967) advanced the doctrine of reasonable expectation to privacy: subjective expectation of privacy as pertaining to privacy. The other objective expectation is that of privacy interests that society acknowledge as legitimate expectations of privacy. The *Katz* case safeguarded areas of personal expectations of privacy, as protected by 4th Amendment interests. This landmark decision was a victory, along with *Berger* and Title III.

Significantly, in respect to the FISA Amendments Act (2008), and the Restore Act (2007), there were restrictions placed on warrantless wiretaps in respect to location. The Senate and the House both passed Protect America Act (PAA) in 2007. However the PAA was only authorized for 180 days and would expire in Feb. 28, 2008. Prior to the PAA, no prior court permission was required to spy on communications between foreign targets of surveillance, even if the communication passed through the U.S. However, a warrant was required to spy on communications between foreign targets and Americans. (www.sourcewatch.org/index.php?title=RESTORE Act_(2007_FISA-bill)

The following are general provisions of the Restore Act. There were two versions of the bill formulated in the Senate. This was first passed by the Intelligence community, which grants immunity to telecom community companies that assisted the government in warrantless surveillance activities. The second version adopted by the Judiciary Committee, strengthened civil liberties protection and stripped telecom immunity. The Senate Intelligence Committee version of the Bill passed in 2008.

The provisions allow warrantless spying on foreign-to-foreign communications passing through the U.S., and tighten warrant requirements for spying on foreign-to-American communications. After obtaining the order from the Foreign Intelligence Surveillance Court, the Director of National Intelligence could then authorize wiretapping on those targets without obtaining individual probable cause warrants for the court. Several restrictions were placed on "basket warrants." The US Attorney General and the Director of Intelligence would have to certify that the purpose of the surveillance was to gather intelligence from foreign targets, even if spying on Americans was involved. The court would review the targeting procedures and verify

that information on a non-suspect American to prevent "reverse targeting." Also, more foreign target suspects would be monitored under intelligence than American citizens.

The U.S. Attorney General and the Director of National Intelligence would also have to specify how much communication with Americans would be collected before a regular warrant was required. The Restore Act provided for oversight governance for foreign intelligence gathering by the Department of Justice and Congress. The Act prohibits warrantless physical searches outside the U.S. (www.sourcewatch.org/index.php?title=RESTORE Act_(2007_FISA-bill) There was a portion of the bill with subpoena power to investigate The Bush administration's warrantless spying program. However, ultimately, amnesty was given to the telecommunications company alleged to have broken privacy laws.

However, the threat of terrorist attacks led to a change in the amount of time permitted for warrantless searches from the 48 hours FISA (1978) originally allowed to seven days in the FISA Amendment Act of 2008. It also removed requirements for detailed descriptions of the property targeted by the surveillance. Another changed prohibited a foreigner from eavesdropping on an American's call or e-mail without court approval. The program allowed the FISA Court 30 days to review existing but expiring surveillance orders before renewing them. It allowed wiretaps in emergencies without court approval, provided the government files required paper work. Importantly, the program prohibited the government from invoking war powers or authorities to supersede surveillance rules in the future. The Act allowed the government to conduct 148 hours of surveillance in a week without a warrant, increased from 48 hours of the FISA (1978), as long as the FISA Court is notified, at the time, of when the surveillance is being conducted, as the FISA Court must review the request in 168 hours. (www.ny.sun.com/national/senate -grants-companies-immunity/81825/)

3.5.3 Intrusion

There has always been a covert means of intrusion though the Title III provision, which permits the lack of notice when conducting telephonic surveillance in certain situations (Lafave et al, 2004). Interception without prior judicial authorization is permitted when there is a designated enforcement officer who reasonably determines that an emergency situation exists with (i) immediate danger and death or serious physical injury to any persons, or (ii) conspiratorial activities of organized crime. In such cases, wire, oral and electronic communication (3.3) may be intercepted before an order authorizing such interception can be obtained.

3.5.4 Information Acquired

The wiretap statute in *Berger* required very little way of the conversation. (LaFave et al, 2004). The Court held that this did not meet the 4th Amendment requirement, and that in order for the communicational content to be seized, it would have to be described and specified. However, Title III established the statutory procedure and guidelines for both Federal and State police agencies to acquire wiretap content, so as to attempt to deter any abuse.

However, there is stark difference between communicational content and addressee information. In *Smith v. Maryland* U.S. 735 (1979), the Court ruled on numbers traced from dialed numbers through a pen register by the police. Phone numbers do not constitute "communicational content" and hence the surveillance of them is not entitled to 4th Amendment protections.

3.5.5 Consent

LaFave et al (2004: 236) describe an important exception to usual Title III procedures, and that is the requirement when an interception occurs only pursuant to a court order involving

one party in a communication. The Act specifically provides that it "shall not be unlawful under the color of the law to intercept wire, oral or electronic communication, where such person is party to the communication or one of the parties to the communication or one of communication or one of party to the communication, where such communication has been given prior consent to such interception."

3.5.6. Notice

Since the *Berger* and *Katz* decisions, requirements for judicial and administrative oversight have greatly strengthened privacy protection in Fourth Amendment law relating to telephonic surveillance. Prior to these cases, according to LaFave and Israel, there were practically no requirements for notice regarding telephonic surveillance. This changed when Congress passed Title III, which supported notice.

3.5.7. Third Parties

There are three alternatives for third party members or persons to involve themselves in telephonic surveillance (LaFave et al, 2004): 1) by having the consenting party wear or carry a tape recorder where he records the conversation; 2) by having agents equip the consenting party member with a transmitter; and 3) a sting operation.

Under Title III as it relates to third-party interception, it must be assessed under a special provision declaring that it was not lawful "for an operator or switchboard, or an officer, employed, or agent of wireless electronic communication services, whose facilities are used in transmitting wire or electronic communication, to intercept, disclose, or use that communication in [his] normal course of employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights of the provider of the

services." (LaFave et al, 2004). FISA Amendments Act (2008) also prohibits the individual states from investigating, sanctioning, or requiring disclosure by complicit telecommunication companies. That law protects telecommunications companies from lawsuits for "past or future" cooperation with federal law enforcement authorities, and the law assists the intelligence community in monitoring terrorists by granting immunity to complicit telecommunication companies.

3.5.8. Investigational Purposes

The investigational purpose of telephonic surveillance is to monitor threats to public safety, national security and threats from organized crime. Since *Berger,* Title III, and *Katz,* there has been advancement in privacy protection under the 4th Amendment, as reflected in their strong suppression remedies and penalties against police abuse of power.

3.5.9 Remedy

Title III includes a statutory suppression of evidence clause in cases where electronic eavesdropping does not meet these requirements of the 4th Amendment. (LaFave et al., 248) Evidence suppression must follow on the basis of these provisions if the communication was unlawfully intercepted.

Suppression is imposed when the order of the authorization or approval under which a communication was intercepted was not a legitimate interception, and was not made in conformity with the order of authorization and approval.[3] The significance is that Title III was enacted by Congress with remedial privacy protections against illicit wiretapping, according to the 4th amendment.

[3] See *Giordano v. U.S.* 394 U.S. 310 (1969); *US v. Chavez* 416 U.S. 562 (1974)

Chapter 4

General History of Cyber-surveillance, Cyber-Crime, and Cyber-Terrorism in the U.S.: 1990's - Present

The expansion of global informational technology resulted in the emergence of cyber-crime in the late 20th Century. The majority of the crimes committed in cyberspace are commercial crimes. Commercial markets in North America, Europe and Asia Pacific were expected to grow to $9.5 trillion dollars, or about 93% of the world wide total. (Ebershoe, 2000)

Criminal offenders exploit network vulnerabilities to pursue their ends. There are numerous ways in which these vulnerabilities can be exploited for illicit gain. The FBI estimates that electronic intrusion causes a loss of $10 billion every year within the U.S. alone (Merl, 2001, Sager et al., 2000). The total annual financial loss due to cybercrime between 1997 and 2002 increased 450% totaling $1,459,755,245, according to the CSI/FBI Survey. (2002) Internet fraud and scandals have therefore become a significant problem. Losses from the Internet through civil fraud were from $198 million in 2006 to $239 million in 2008. (www.securitywatch.co.uk./2008/04/04/the-latest-cybercrime-statistics/). Much of the major damage in fiscal and information technology comes from malware and malicious viruses. (Markoff, 2008).

In respect to international terrorist surveillance programs, Taliban and Pakistani spies have used electronic surveillance in conducting their operations. (Mazzeti and Schmitt, 2009) The Chinese government has infiltrated into 4,295 worldwide governmental computers. (Markoff, 2009) And during the following summer, the North Korean government hacked into the U.S. Pentagon, and S. Korea's Central Intelligence Agency.

Vulnerabilities exist for cyber attacks on government, military, infrastructure and commercial institutions, and the damaging effects can be completely disastrous. This is because these attacks can remain unidentified in the Internet through the course of the attack. This being the case, it has seen been said, "the boundaries between cyber-warfare, cyber-crime, cyber-terrorism have been blurred. (Wilson, 2008)

Wilson summarizes his report linking with these opening remarks on the transnational dimension (CRS Report RL 32112).

Cybercrime is becoming more organized and established as a transnational business. High technology on line skills are now available for rent to a variety of customers, possibly including nation states or individuals and that could secretly represent terrorist groups. The increased use of automatic attack tools by cybercriminals has overwhelmed some current methodologies and for tracking cyber-attacks, and vulnerabilities of the U.S. critical infrastructure, which are acknowledged in publications, could possibly cyber-attack to extort money, or damage the U.S. economy to the affect the national security.

Wilson illustrates the cyber-attacks on the Estonian government in 2007 and their military, economic, and infrastructural institutions by Russia. He also observes that Al Qaeda uses the most complex telecommunication and digital tools to communicate with their group.

Wilson (2008: 4) cites several definitions of cyber-terrorism and cyber-crime. Dorothy Denning (2001) defines cyber-terrorism as "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage." The Federal Emergency Management Agency (FEMA) defines cyber-terrorism as "unlawful attacks and threats of against computers, networks, and information stored therein when to intimidate or coerce its people in furtherance, of political or subjective objective."

If a terrorist group were to make a cyber-attack for the mentioned reasons above, it would be both an act of cyber-terrorism and cybercrime.

As Wilson (2008:15) claims, the association between cyber-terrorism and cyber-crime is hard to determine. However there is a nexus. For example, in the UK in 2005, the bus and subway bombings and the attempted car bombing in 2007 provide evidence that terrorists are secretly active "within countries with large computer infrastructure and network communications" and they can clandestinely communicate. It is reported that these criminals communicated with terrorist groups in Eastern Europe.

The Department of Defense uses Commercial Off the Shelf (COTS) hardware and software products in core information technology administrative functions, and combat functions, and also in tactical systems of all services for the military (Wilson, 2008: 24).

Given the limited level of security protection in commercial software, there is no way to fully secure the vulnerabilities of network information systems. In addition, there is no foolproof way to surveil and identify the hackers who intrude into computer systems. This is why cyber-attacks are highly successful from reading Wilson's analysis (2008: 24).

Wilson further says that Computer Emergency Response Team/CERT has abandoned its traditional practice of monitoring network intrusions by business and establishments worldwide. CERT abandoned such practice because "the number of wide spread use of new, automated cyber-attack tools had escalated the a number of network attacks to such a high level, that CERT/CC organization determined that that traditional methods of counting security intrusions had become meaningless as a system." (Wilson, 2008: 28).

The very last problem is tracing cyber-crime and cyber-terrorism. Financial, and military and governmental institutions that have been damaged by cyber-criminals and cyber-terrorists have not revealed the damage. However, the Chinese and Russian governments wage a cyber-

warfare on U.S. governmental and military network data banks. (Sanger, Markoff, Shanker, 2008).

4.2. Post 9-11 Federal Administrative and Agency Responses to Cyber-crime and Cyber-terrorism

In 1998, President Clinton approved the Presidential Decision Directive 63, which established a Federal framework for national critical infrastructure protection measures. Central organizations were created: FBI National Infrastructure Protection Center and Cyber Division, and the Critical Infrastructure Assurance Office located in the National Security Council. The Infrastructure Threat Assessment has joined Infraguard, a business-controlled organization. The Homeland Security Act was enacted to respond to the alleged threat of increasing attacks. After the 9/11 attacks it has been said that the government and private network faced new threats of terrorist attacks, such as attempts to bring havoc to major financial centers, transportations, and utilities. A day after 9/11, the Senate Governmental Affairs Committee determined that governmental and other infrastructures were vulnerable to an attack. The significant threat to homeland security, electronic commercial markets, and telecommunications from criminals and criminal enterprises and terrorists remains a problem yet to be fully addressed on a systemic, organizational level.

Since then, more has been done by the Federal government to protect the U.S. from cyber-attacks. In 2002, the Federal Information Security Management System (FIMSA) was established, giving the Office of Management and Budget the responsibility for overseeing and regulating the information security standards and guidelines developed by federal agencies (GAO, 2003).

Moreover, the National Security Division (NSCD) within the National Protections and Programs Directorate and Department of Homeland Security manages a Cyber Security Tracking, Analysis and Response Center (CSTARC) (Wilson, 2008:31). At the moment, it is uncertain whether the NSA will take control of these cyber-security functions, and centralize aspects of management of the Department of Homeland Security under the proposed Cyber Security Act.

4.3. Typology of Cyber-crimes

In addressing the type of cybercrimes committed in the U.S. and abroad, various types of crimes have been distinguished. Below is a typology of criminal offenses (Putnam and Eliot, 2001: 38: Power 2000:4).

- Unauthorized access into information network systems.
- Illicit tampering with files or data (unauthorized copying, modification or destruction.)
- Computer network sabotaging (e.g. viruses, Trojan horses, denial of service attacks, and etc.)
- The use of computers to commit traditional crimes (e.g. terrorism, money laundering, fraud, forgery, prostitution, narcotics.)
- Computer mediated espionage (e.g., theft of secret financial, political, and military secrets).
- Violation of privacy in acquisition of personal data.
- Theft or damage of computer hardware or software.
- Identity theft.
- Software piracy.

Kovacich and Boni (2000) also describe cyber-terrorist activity, and they have formulated the following typology:

- Use of computers to penetrate a control tower computer system and send false signals to aircraft, causing them to crash;
- Use of fraudulent cards to finance operations; or penetrate a financial computer system and divert millions of dollars to finance their activities;
- Use of cloned cellular phones over the Internet to communicate using encryption to protect their transmissions; and
- Use of virus and worm programs to shut down governmental agencies; or penetrate computerized train routing system, causing passenger trains to collide, or take over telecommunications links or shut them down.

Clearly, it is important to realize that cyber-surveillance tools can monitor these criminal activities with a minimum amount of intrusion of privacy.

Global cyber-terrorism is made more challenging by the universal access to the World Wide Web that is available to rogue states, terrorists, rival national sovereign states, the military, cyber-organized crime syndicates. With ECHELON surveillance, U.S. Military crypotological networks can be decrypted by hackers, and global internet networks render any institutional agencies vulnerable to attack.

Lukas (2001: 181) remarks on the prospective uses of defending against attacks and vulnerabilities: "A threshold issue for considering long-term changes in information systems will be that of weighing the cost of ignoring cyber-attacks against the cost of action to reduce the severity and frequency of failures." Lukas understands the threat of global cyber-terrorism and cyber-crime as a paramount risk and uncertainty.

Ch 5. Carnivore:

A Case Study on Cyber-surveillance

5.1 Carnivore: Technical Description and Overview

Carnivore, which is no longer in use, was introduced by the FBI in the 1990's as a Microsoft Windows based e-mail filtering program. Carnivore was operated through a workstation connected via telephone network to the main Carnivore system located at the Internet Service Provider's (ISP) headquarters (Georgiton, 2001). Carnivore had no monitor or keyboard, and was enclosed in a black box connected to the ISP, working as a filter, as a "packet sniffer." Carnivore initiates a search, which can include Internet ports, specific Internet Protocol (IP) Addresses, Simple Mail Transfer Protocols (SMTP) and Post Office Protocol (POP 3) addresses, individual usernames for particular Internet or e-mail account, and specific text strings contained in the e-mail. After the filter criteria are established, the Carnivore program is processed in the FBI's office, linked to the computer located next to the ISP's program, monitoring the targeted e-mails. (Georgiton, 2001; 3). It is inconclusive whether Carnivore ever achieved the full capacity to monitor entire e-mail traffic, to monitor targeted e-mails or to target random e-mails.

According to ECPA, Congress realized that the procedural requirements for telephonic wiretap and e-mail intercepts are not similar. "It is impossible to 'listen' to a computer and determine when to stop to listening and minimize it as it is possible to do in listening to a telephone conversation." (Fishman and Mckenna, 1995) No federal court has considered the minimization procedure to the interception of e-mail, due to the mechanical and technical aspects of how such a minimization process would be performed. Therefore, a problem raised by

Carnivore was the principle of minimization (Kerr, 2007, http://volokh.com/archives/archive_2007_02_04-2007_02 10.shtml#1170708253). The need to "minimize" (how broad or narrow the search in terms of people monitored; the duration of the e-mail tap, and the number of targets, surveilled or to be surveilled) remains a question, which could not be conclusively answered in regard to how Carnivore was being utilized.

5.2. History and Deployment of Carnivore

Carnivore was used in the mid to late 90's and was officially abandoned in 2003. Its use was heavily criticized due to the possibility of intrusion on civil liberties and privacy protections, along with operations that would monitor e-mail traffic. Cyber-surveillance technology may be cause for concern with respect to issues of privacy because cyber-surveillance technology, in general, is the latest surveillance technology used by law enforcement agencies and has become more intrusive than the previous technologies (Etzioni, 2003). However, proponents believed that there was great difficulty investigating and monitoring cybercriminals without the use of intrusive cyber-surveillance tools.

Some have surmised that Carnivore was a version of a packet sniffing software tool known as Etherpeek. Those who were target(s) of surveillance may not have been suspects of an investigation or a crime.

E-mail may be randomly searched by Carnivore to intercept incriminating evidence. As Geofrey North (2002: 17) writes: "Carnivore may have the ability to impound all electronic information, then filter out those that do not give rise to investigation." Carnivore was very much a sophisticated "packet sniffing device" installed (at a point of access) to an ISP. The question of how Carnivore limited its search remains undisclosed. But some argue that though Carnivore reads all the e-mails in traffic that move through the ISP server, it has the capacity to limit the

search by targeting words, e-mails, addresses, a string text of words (as in the header and/or content), that may be specified in the warrant. Therefore, if the targeted words, string texts, or e-mail address are not detected by the filter, the e-mail will be disregarded.

In the past decade, in response to the expansive growth of cybercrime and threat to national security by cyber-terrorism, fraud, child pornography and transnational organized crime, the FBI developed such tools as Carnivore and Magic Lantern to combat such activities. Although most internet communication is benign, the use of e-mail by high profile terrorist organizations continues to grow at an alarming rate.

In the past two decades there has been a series of attacks on the computer networks of businesses, banks, civil institutions and governmental agencies. It is known that the members of Al Qaeda communicated through the use of encrypted e-mail prior to and during 9/11.

In response to the growing problem of cybercrime, Louis Freeh (1997:2) former FBI Director, testified to the Senate Judiciary Committee: "The explosion of technologies and the globalization of crime have become realities. The need for right investigative tools is immediate…..information must flow unimpeded and coordination at all levels must be superb if we are to continue making inroads against these increasingly complex crimes."

Freeh also claimed that the new surveillance technologies must be implemented and deployed by law enforcement to effectively investigate and prosecute cybercrime, as well as to gather intelligence on terrorism in a post 9/11 period. Freeh argues that we may be warranted in believing that technological advances have created serious problems, so that combating and preventing cybercrime and cyber-terrorism must become one of federal, state and local law enforcement's greatest priorities. Law enforcement needs to implement and utilize new computer

investigative techniques to confront the already pervasive threat and the growing problem of cybercrime.

5.3. Technical Means for Agency and Judicial Monitoring

Little judicial supervision and oversight exist pursuant to ECPA, which would apply to how Carnivore is being used. Due to this lack of supervision and oversight, there is little oversight over how FBI agents carry out cyber-surveillance activity, and whether other investigative techniques "could be utilized before resorting to an electronic intercept, or whether the surveillance is necessary." (Fishman and Mckenna, 1995).

Georgiton (2001: 12) makes a very interesting note on judicial supervision and oversight in respect to electronic surveillance: *"*Judicial supervision is not even required for intercept orders, and appellate courts as a rule do not review the adequacy of progress reports or suppress evidence for failure of a judge to require progress reports."

The Supreme Court established a "reasonableness" standard for privacy relating to minimization according to Title III. Moreover, since enactment of the Title III requirements, there was no judicial supervision or oversight during a Carnivore search, for there was no assurance that the FBI was complying with the intercept order.

5.4 Legal Implications

The question of the 4th Amendment's protection of "unreasonable search and seizure," is a perplexing one. Whether the Supreme Court's decision in *Katz*, which had established the "two prong test" regarding e-mail tapping of Carnivore, can be made the rule for cyber-surveillance activity remains a controversial topic. The first prong is a subjective test of whether or not the person has an actual expectation of privacy. And the second prong tests whether or not society protects such an expectation of privacy. A warrant is required with probable cause, and a

magistrate's review for an e-mail tap, which does not exclude "pen register" surveillance. All that is needed for an e-mail pen register is "reasonable suspicion" and a court order. As Georgiton (2001: 5) writes, "Taken together, the question asked is whether the person observed has a reasonable expectation of privacy?"

Significantly, the Supreme Court has not decided on an answer to questions regarding e-mail taps, or on-line pen register surveillance, and whether or not there is a "reasonable expectation of privacy" in e-mail accounts such as personal and work related.

5.5 Status of Personal Privacy

Carnivore was disbanded after there was enough political repercussion in Congress showing it was extremely intrusive to privacy. There was no way for the public to know exactly how Carnivore was being utilized as stated previously.

Chapter Six

Magic Lantern: A Case Study in Cyber-surveillance

6.1. Magical Lantern: Technical and Overview Description

Magic Lantern, installed in the target computer drive through a Trojan virus, became publicly known to the public in November 2001. Because the software operations of Magic Lantern, as a surveillance tool, are so secretive, "there is a great degree of uncertainty, regarding whether the program would transmit keystrokes of records back to the FBI over the Internet or store information seized in a raid." (Hartzog, 2002).

Magic Lantern may not be an innovation, as private companies have used commercial "KLS"-Key Logger Stroke Systems to monitor e-mail employee e-mails. The significance of Magic Lantern is that its goal is to retrieve e-mail messages, where targeted suspects were encrypting the messages. This is the primary purpose of the Magic Lantern, to record the e-mail messages covertly. Magic Lantern even records passwords that the targeted use to encrypt messages or software.

6.2. History and Development of Magic Lantern

Much of the development of Magic Lantern is classified information. But what can be inferred is that its development began with techniques from malicious codes of various "trojan viruses." The FBI was experimenting with Trojan viruses to target suspects and offenders, to discover criminal information.

The remedy to malicious viruses is the special Anti-Virus programs that have developed, and are still developing, to prevent such Trojan viruses from being installed in one's host computer. Magic Lantern is not a fully reliable software surveillance device.

6.3. Technical Means for Agency and Judicial Monitoring

Like Carnivore, there is little judicial supervision or oversight as to how Magic Lantern is monitored other than the legal requirements for probable cause, such as requirements for judicial permission to proceed with intrusive surveillance, based on the situation not the surveillance technique.

6.3. Legal Implications of Magic Lantern

An additional legal complication regarding Magic Lantern is that it does not fall under the conception of "wired communication," "electronic intercept" or "electronic storage," and "aural transfer," under ECPA. So the problem of classifying it as operative surveillance tool remains a problem. It would then seem, as Hartzog (2002) writes, that Magic Lantern would not be under the supervision and authority of Title I of ECPA (which deals primarily with wiretaps) since it involves "off-line communications."

For example, in *US vs. Scarfo,* 533 U.S. 27 (2001) the court ruled that "FBI did not install and operate any component which would search for and record data entering or exiting the record from the transmission pathway through the modem attached to the computer" because the "FBI configured the KLS to avoid[4] electronic communication intercepting electronic communications typed on the computer and simultaneously transmitted in real time via the communication ports." The Court argued that the KLS did not record any key strokes while the modem operated. Therefore, the FBI did not decode Scarfo's encyption, but used a Trojan virus to get a password for encryption.

It is a matter of dispute and controversy whether or not Title I of ECPA can be interpreted to cover Magic Lantern, because it records key logging strokes falling under the

[4] See Robert Pikowsky, "The Need for Revisons to the Law of Wiretapping and Interception of EMAIL," 10 Mich. Telecomm. Tech. L. Rev. 1, 2003.

rubric of lawful interception, or whether or not it can be interpreted as stored electronic communication.

6.5. Status of Personal Privacy

In the case of Magic Lantern, it is hard to determine its impact on the status of personal privacy. There are no procedural or operational limits, which can be placed with legal or judicial oversight on Magic Lantern because it is used secretly, therefore making it difficult to determine the extent to which it poses any violation of our 4th Amendment rights. However, some privacy protection may remain based on the technical limitations of the software itself and the evolving capacity of anti-virus software to prevent its installation.

Chapter Seven

NARUS: A Case Study of Cyber-surveillance

7.1 NARUS: Technical Description and Overview

NARUS is a commercial e-mail traffic analyzer, a software application that runs on standard IBM or Dell computers, connected to LINUS Network operating systems. It has the ability to monitor digital traffic at a very rapid pace on high-bandwidth pipes, indentifying e-mail packets. It is used by government and private corporations to monitor e-mail traffic within their sectors.

Internet companies can install NARUS at every entrance and exit point of their networks. NARUS communicates with central "logic" servers running specialized applications (Poe, 2006). Poe further states, "The combination can keep track of, analyze and record nearly every form of Internet communication, whether e-mail, instant message, video streams, or VoIP phone calls that cross the network."

7.2 History and Development of NARUS

NARUS was launched in February 2005, and is marketed and supported by a multi-national corporation. The history of the development of this surveillance technology remains a trade secret. There is no explicit or open source information as to how it was developed by network computer systems engineers.

7.3. Technical Means for Agency and Judicial Monitoring

Since NARUS created a large quantity of surveillance tools targeted at large streams of information, and since not much is known about how the tools actually work, it is hard to differentiate between those who have and have not been surveilled as targeted populations.

Therefore, the precise application of consent requirements and other oversight mechanisms is impossible.

7.4 Legal Implications of NARUS

Because NARUS is a new and very advanced cyber-surveillance tool, it is not clear how existing legal requirements for surveillance monitoring would be applied to this new technology. New laws and policies may be needed to regulate the technology.

7.5 Status of Personal Privacy

One of the most pressing concerns with this cyber-surveillance tool is that there is no internal auditing of the NSA. NARUS is the most powerful private cyber-surveillance device used by the government, which can target millions of people at one time. Personal privacy is a risk because a) the technology is not understood, and b) who the technology is being applied to is not understood, and c) the laws that might apply to this technology are not written to clearly cover it, and d) the agency that would be authorizing its use does not appear to be internally auditing its use.

Chapter Eight

Cyber-surveillance and the Status of Personal Privacy

8.1. Overview

This chapter applies the 9-factor rubric to assess the state of personal privacy with respect to the three cyber-surveillance cases. The three tools discussed raise issues of definition and application, so that depending on how the tool is understood or described, it is possible to short-circuit ECPA and related court decisions. The operation and reach of these tools are neither clear nor precise as they are in the *Katz* doctrine of privacy expectations, or in the post-*Katz* jurisprudence where they are justified in respect to computer surveillance procedural law, policy and oversight.

8.2.2. Location

Carnivore and NARUS are deployed by mass telecommunication companies, which then enable authorized agents to monitor e-mail communication and interceptions through electronic surveillance. However, it is unknown how Magic Lantern operates since it is done covertly to monitor key logging strokes.

8.2.3. Intrusion

Bradford Councilman's case is the most controversial case of interpretation and application of ECPA in regard to the Wiretap Act (Title I) and Storage Communication Act (Title II). Councilman was convicted of intercepting mail from Amazon.com for his advantage. However, Councilman argued that "Congress considered communications in computers to be worthy of less protections in wires because users have less expectation of privacy for electronic communication." He further argues that after the wire transmission, and when the message is

stored in computers, ECPA, in respect to Title II, provides less protection because it is electronic communication.

The category of electronic communication added to the ECPA statute did not impose the same level of review as for telephonic wire protection, which is oral communication (LaFave et al., 2004: 231).

However, the court argued, by citing the Office of Technology Assessment Report (www.ws. Princeton.edt/~ota/disk2 /1985/8509_n.html) on Electronic Surveillance and Civil Liberties, that the broad definition of electronic storage "sought to ensure that the message and bi-product files that are left behind after transmissions, as well as messages stored in the user's mailbox are protected from unauthorized access." (OTAR, 48-49). The court rejected Councilman's argument and concluded by reasoning that the "term" electronic communication includes transient electronics that are intrinsic to process this form of communication. The court finally concluded that "temporarily stored e-mail messages at issue here constitute electronic communications within the scope of the Wiretap Act, [in which] the statute also requires the conduct alleged in indictment to be an "interception"[5] 18 U.S.C. 2511(2) (a) (i). Title I puts the ISP on notice of both prohibited conduct and the narrow provider exception, of what it can do. The court deemed the provisions of the Wire Tap Act to constitute adequate notice.

Title II is less stringent in its requirement for a search than the Wiretap Act. Regular warrants are required to obtain the contents of electronic storage in 180 days or less. If communications continue over more than 180 days, the state can access them with an

[5] The court writes : "Even we conclude that temporarily stored e-mail messages at issue here constitute electronic communication within the scope of the Wiretap Act, the statute also requires the conduct alleged in the "indictment" to be an interception", U.S.C. 2511. The offenses are as follows: intentional intercepting of e-mail, or to procure any other person to intercept. pp.26-27.

administrative subpoena, a grand jury subpoena, a trial subpoena, or a court order. (Solove, 2004) There is no requirement for probable cause.

With respect to intrusion of e-mail by mass surveillance, *Hepting v. ATT*, 441 F. Supp. 88992006) is a controversial case. The Plaintiff Hepting claimed that the NSA illegally tapped American's private communication through ATT. ATT was named because it collaborated with the government, without a warrant, to surveil vast populations of American citizens. NSA claimed state secret privilege as its defense against the law suit. The Federal appellate court determined that the case would proceed; but that with the passing of FISA Amendments Act (2008) retroactive immunity would be given to telecommunication companies.

The second similar case is *Jewel v. NSA,* and other governmental agencies on behalf of ATT customers to stop what they viewed to be illegal, unconstitutional, and dragnet surveillance of mass telecommunications. In 2009, the United States filed the Government Defendant's Notice of Motion to Dismiss for Summary Judgment. The government argued that a) Congress has not waived sovereign immunity for the plaintiff's statutory claims; b) Congress has expressly preserved the sovereign unity for ECPA and FISA; and c) Congress supports the state secret's privilege to a non-disclosure policy and operational regulation.

While this case has not been decided, for the government to present this as its legal position is a very significant setback for personal privacy protections.

8.2.4. Information Acquired

This is a complex question that involves issues of content, address information, header, and target population, or mass surveillance population, when e-mail is intercepted. Moreover, there are no extensive rules for minimization of electronic communication, and the FISA Amendments Act (2008) rules are governmentally classified information.

Pen register surveillance is not protected by the 4th Amendment. Under *Smith v. Maryland,* 442 U.S. 735 (1979), Fourth Amendment protections do not apply to pen registers that capture the numbers dialed from a particular telephone, as opposed to the content of telephone conversations. The principle that the Fourth Amendment protects against the acquisition of contents, but not addressing information, was extended to electronic communications in *United States v. Forrester,* 512 F.3d 500 (9th Cir. 2007), which held that neither email addressing information nor the IP addresses of websites accessed from a particular email account were subject to Fourth Amendment protection.

8.2.5 Consent

Title I defines the terms of consent for disclosure of information acquired. Section 2511 (3a) of Title 18 defines several provisions about consent: "A person or entity providing an electronic communication to the public shall not intentionally divulge the contents of any communication (other than such person or entity, or an agent thereof) while in transmission on that service to any entity other than the addressee or intended recipient of such communication or an agent of such addressee or intended recipient."

Moreover, a person or entity providing electronic communication service to the public may divulge the contents of the communication with lawful consent of the originator or the intended recipient. The content can also be divulged to a person employed or authorized, or whose facilities are used to forward such communication, or which was inadvertently obtained by the service provider and which appears to pertain to a crime.

8.2.6. Notice

Notice is a legal procedure obtaining court approval for an action proposed by a government agency. Section 2518(3)d states the application for an interception must contain a

full and complete statement of the evidentiary basis for surveillance of those alleged to be committing the crime. Section 2518(11) (b) states. "A provider of wire or electronic communication service that has received as provided may move to court to modify or quash the order on ground that its assistance with respect to the interception cannot be performed in a timely or a reasonable fashion. The court upon notice to the government, shall decide such motion."

8.2.7. Third Parties

U.S.C. 2701 (1) states in respect to Title II that it is illegal to access without warrant wire, oral or electronic messages.

In matters concerning subscriber information, a person or entity providing remote computing services to the public shall not knowingly divulge to any persons or entity the contents of any communication which is received, carried or maintained at the service on behalf of a subscriber or customer.

There are several exceptions. A person or entity may divulge the contents of a communication:

- to an addressee or intended recipient of such communication or an agent of such addressee or intended recipients,
- with lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing,
- to a person employed or authorized or whose facilities have received such communication;
- to a law enforcement agency, if such contents were inadvertently obtained by service provider, and pertain to a commission of crime,

A provider of electronic communication services or remote computing services may not disclose a record or other information pertaining to a subscriber or a customer of such service or to any person other than a duly authorized governmental authority.

The government can disclose contents under an administrative subpoena by Federal or State statute. This is important when the subscriber gives consent to the service provider. However, under approved court orders, a governmental entity receiving records or information under Federal and State subpoena is not required to give any subscriber or customer notice. There are no restriction placed on ISPs providing content information when it is accord with a court order, warrant and subpoena under Title II.

In *Freedman v. America Online,* 412 F. Supp. 2nd 174 (D. Conn. 2005) the issue of a subscriber's claim to reasonable expectation of privacy was decided against the Plaintiff based on ECP; that subscriber is not entitled to non-disclosure of content by ISPs when a warrant or subpoena is issued by the government.

8.2.8. Investigational Purposes

The goals and objectives of surveillance are intrinsic to the justification of cyber-surveillance in any case. The general purposes of preventing and stopping cyber-crime and terrorism are general invoked. ECPA and FISA Amendments Act (2008) are the Federal Statutory Acts which have applied during the past thirty years as regulatory and oversight policy for investigation and intelligence purposes for Federal, state, and local police agencies.

8.2.9 Remedy

Orin Kerr (2003:2) states the case for a suppression remedy as tantamount in principle to the exclusionary rule for illegal e-mail interception. However, at present there is no such

suppression remedy for electronic communication, in contrast to the law of wire communication where the suppression remedy is available to the court.

Kerr further argues that Congress should "reconstruct the remedies scheme of Internet Surveillance by statutory suppression remedies for violations of Internet surveillance statutes." In sum, Kerr argues that there needs to be a balance between Internet privacy and the rule of law enforcement, and intelligence agencies should not abuse their power through illegal searches.

Chapter 9.

Assessment

9.1. Privacy Protections in Light of Cyber-surveillance, Technology and Law

The ebbs and flows of the history of surveillance and cyber-surveillance have always surfaced in periods of crisis and in times of threat to national security. There was a great expansion in the interception of mail during the American Revolutionary War, and Civil War, and during World War I, as there was a perceived threat to national security by domestic political subversive groups. During World World II and the Vietnam conflict, the interception of mail involved the seizure of intelligence information that would help to defend the nation. .

The *Katz* case and Title III, ECPA, FISA, USA PATRIOT ACT, RESTORE ACT, FAA and, the recently proposed Cybersecurity Act, each was intended to protect expectations of privacy while restricting authorities from the abuse of power. However, in times when there is a struggle to balance personal privacy and civil freedoms with the need to protect the nation from terrorism and disorder, the radical advancement of cyber-surveillance technology negates liberal democratic freedoms such as privacy.

The case studies about Carnivore, Magic Lantern, and Carnivore each included instances governmental actions and procedures in which the protection of personal privacy was indecisive, unclear, and undefined, other than Title III, Patriot Act, and FISA and the Fourth Amendment. The procedural oversight of cyber-surveillance policy and practice is very much in doubt in the ongoing contest between national security and personal privacy.

The operational or policy goals and objectives of the three cyber-surveillance tools remain very similar in that they seek to achieve surveillance of mass populations. The three cyber-surveillance tools each would erode personal privacy protections, in the interest of

promoting national security, at least alleged by the government. The surveillance and cyber-surveillance in the governmental sector and private sector remain covert and are protected by federal trade secrets law by global telecommunication corporations.

9.2. Lessons From the History of Surveillance or Cyber-surveillance

Since American colonial time, the law of postal mail privacy has not changed. For example, the limits of the law regarding the correspondent U.S. Code has not changed in respect to the "sanctity of sealed mail" other than the conditions of threats to national security and subversion.

As for electronic telephonic surveillance wiretap, the limits of the law under TITLE III, was amended by ECPA and CALEA. There were strict minimization requirements which applied to the person or group being wire-tapped.

In contrast, the greater technological capabilities of cyber-surveillance, as well as difficulties in formulating oversight and monitoring, led to the controversial rulings of the Hepting case, Jewel vs. NSA which has not been dismissed, Restore Act and FAA (2008) and the government's attempts at sovereign immunity and warrantless telecommunication searches.

9.3. The Status of Personal Privacy

The two leading cases relating to cyber-surveillance are Hepting v. ATT, and Jewel v. NSA. The EFF brought two civil suits against ATT and NSA, alleging that millions of ordinary American citizens, were being warrantlessly monitored under President Bush's TSP Program. ATT was given retro-active telecommunication immunity, and the case did not win in court based on the provisions of FAA (2008).

Jewel v. NSA has yet to be heard. But the issue in both cases is that government has claimed state secret privilege on the grounds that terrorist surveillance required data mining

operations to identify "names, identities, and places" and that nothing more could be disclosed other than this basic information, because it would jeopardize domestic and foreign intelligence operations. Hepting has amended another complaint claiming the violation of separation of powers between the judiciary and the provisions of the FAA.

The issue here is that mass monitoring of random-targeted populations jeopardizes the 4th Amendment privacy protections and interests. The opposing argument is that we have not developed the technology, or that the technology does not exist to minimize the level of surveillance of mass target populations. A second opposing arguments is that the government does not want to make the data mining source code of TSP programs open to public scrutiny. This argument has previously applies to telephonic wiretap and the opening of mails, as indicated in previous chapters.

4th Amendment privacy protections and interests are at stake. Is there enough evidence on the side of government to show that the U.S. is under a clear and present danger to warrant such en masse monitoring, and continual policy of state secret privilege for postal, telephonic surveillance and cyber-surveillance?

9.4 Conclusion

The primary question of this dissertation involves responses to the emergence of new technologies for communication, and risks and crimes enabled by the new technologies, and the official responses to the new technologies such as cyber-surveillance. How can a balance be struck between the need for surveillance, and the need to preserve 4th Amendment protection and privacy interests.

Privacy must be protected as a paramount and important concern. But as also shown, privacy has been undermined and threatened, and diminished in time of war, social unrest, and high rates of crime. There is now a clear danger that the 4th Amendment is being unlawfully violated by agents of the state.

Federal Regulatory Law and Oversight has been designed to protect privacy interests, but now poses a challenge to 4th Amendment interests. There are no conclusive answers to such issues other than how the courts have decided upon such issues. This through the rest of the status of the privacy factors in this concluding chapter will report the findings of the researcher's analysis in a chronological historical context.

The preservation of personal privacy will depend on how the state responds to perceived threats and risks for terrorism and cyber-warfare, foreign subversion in the U.S. and abroad. There is no exact way to calculate this perceived threat or risk, beyond the best assessments of experienced public officials, informed by intelligence gathering and analysis.

The ordinary person's expectation of privacy was clear, when there was no threat to national security or rampant crime during the colonial period when privacy was highly protected through postal services, and telephonic statutory laws. The sanctity of mail, and the mail cover protected citizens from unlawful privacy intrusion. In the 1960's, Title III protected those who were under the scrutiny of wiretaps through minimization procedure. However, in the period following the World Trade Center attack, technologies for mass surveillance, and the lack of effective oversight technological mechanisms for cyber-surveillance monitoring eroded privacy rights.

In the nine-factor analysis of privacy applied to each period and case in this dissertation, the comparison of the similarities and differences is significant to understand how cyber-surveillance presents different challenges than traditional surveillance.

- Theory and definition: Cyber-surveillance technologies do not lend themselves to direct comparisons with earlier technologies. Therefore, new interpretations constructions of investigative conduct can be introduced to evade legal requirements clearly applicable to earlier technologies. When new law is fashioned to address the new technologies, protections can be weakened.
- Location: The cyber-surveillance tools have no limits, and are clandestine.
- Intrusion: The investigating agencies operate under FAA rules, and also remain clandestine. Intrusion can be easily concealed.
- Information acquired: The information gathered is protected under the FAA.
- Consent: It is uncertain to the potential targets of cyber-surveillance whether they are the subjects of a surveillance program.
- Notice: The timing and nature of notice is not well-defined or technically practical.
- Third parties: It is classified and not disclosed to the public whether or not a a cyber-surveillance operation is taking place.
- Investigation purposes: These are highly classified and are protected with a non-disclosure policies and practices.
- Legal remedies: Under the FAA, there are no legal remedies for those whose privacy was invaded by clandestine surveillance or cyber-surveillance operations.

Surveillance has always been a tool of governance in times of national emergency. Police actions that intrude on privacy evolved into modern wire and electronic surveillance. After the World

Trade Center attack, one must ask Juvenal's question: "Quis custodiet ipsos custodies?" to challenge the use of governmental surveillance authority, considering the consequences for personal privacy of changes in legal and operational criminal procedure, as well as technological capabilities for surveillance. In the age of global terrorism and cyber-surveillance, citizens must seek a balance between the protection of privacy rights and the need to pursue public order and national security.

Bibliography

Alderman v. United States, 394 U.S. 165 (1969)

Alberti, A. (2002). Wiretaps: a complete guide for law and criminal justice professionals. Ft. Lauderdale: Austin and Winfield Publishers.

Ballard, J.D., Hornik, J.G., Mckenzie, D. (2002). Technological facilitation of terrorism: definitional, legal and policy issues. American Behavioral Scientist, 45,958-989.

Barker, J. (2004). "Comment: Society's carnivore, both good and bad, why we need it, and how to regulate it." 74 UMKC L. Rev. 945.

Benn, S. (1971). Privacy, freedom, and respect for persons. In J. Pennock and J. Chapman. (Eds.) Privacy. (pp.1-27). New York: Atherton.

Bereano, P. (1999). Technology and human freedom. In M.D. Ermann, M.B. Williams, C. Gutierrez. (Eds.). Computer, ethics, society. (pp.278-84). New York: Oxford University Press.

Berger v. New York, 388 U.S.41 (1967)

Borsook, P. (2000). Cyberselfish: A critical romp through a terribly libertarian culture of high tech. New York: Public Affairs.

Center for Strategic and International Studies. (1998, November). Cybercrime……cyberterrorism……cyberwarfare: Averting an electronic waterloo. Retrieved June 1, 2001, from http://www.csis.org/pubs/cyberfor.html

Carol, G. (1997). "Federal agencies open unified hard drive to control mafia." New York Times, February 22.

DeCew, J. (1986) The scope of privacy in law and ethics. Law and Philosophy, 5,145-173.

DeCew, J. (1997). In pursuit of privacy: Law, ethics and the rise of technology. New York: Cornell University Press.

Denning, D. (2000). Statement of Dorothy E. Denning. Retrieved June 4,2001, from http://www.house.gov/hasc/testimony/106thcongress/00-05-23denning.htm

Denning, D. (2001). Information warfare and security. Boston: Addison and Wesley.

Denzin, Norman K. and Yvonna S. Lincoln (eds.) (1994). Handbook of qualitative Research. Thousand Oaks, CA: Sage.

Denzin, Norman K. and Yvonna S. Lincoln (eds.) (1998b). The Landmark of qualitative Research. Thousands Oaks, CA: Sage.

Denzin, Norman K. Yvonna S. Lincoln (eds.) (1998c). Strategies of qualitative Inquiry. Thousand Oaks, CA: Sage.

Ditzion, R. (2003). "Electronic surveillance in the internet age: a strange case of pen registers." 41 Am. Crim. L. Rev. 1321.

Dowley, M. (2002). Government surveillance under the U.S.A. PATRIOT ACT: Is it possible to protect national security and privacy at the same time? A constitutional tug of war. 36 Suffolk U. L. Rev. 165,182.

Douglas, J.D. (Ed.). (1971). The technological threat. Englewood Cliffs: Prentice Hall.

Drozdova, E.A. (2001). Civil liberties and security in cyberspace. In. A. Sofaer and S.E. Goodman (Eds.). Transnational dimensions of cybercrime and terrorism (pp.265-286). Stanford: Hoover Institution Press.

Dunham, G. (2002), Carnivore, the FBI e-mail surveillance system: devouring criminals, not privacy. 54 Fed. Comm. L.J. 543, 566.

Erbschloe, M. (2000). Business on the web is not worldwide. Retrieved July 7, 2002, from http://www.businesseconomic.com/cei/press.index.
index.html

Electronic Frontier Foundation, NSA spying FAQ, http://eff.org./nsa/faq

Ellul, J. (1964). The technological society. New York: Vintage.

Etzioni, A. (2002). Implications of select new technologies for individual rights and public safety. 15 Harv. J. Law and Tech 257. 290/

Etzioni, A. (1999). The Limits of privacy. New York: Basic Books.

Fowler, G. (1977).Unmailable. Athens: University of Georgia Press.
I
Freedman vs. America On Line, Inc. 412 F. Supp.2nd (D. Conn, .2005).

Freeh, L. (1997, June 4). Excerpts from testimony to the senate judiciary Committee. Retreived June 5, 2003, from Center for Democracy and Technology Web site: http://www.cdt.org/digi_tele/970604_Freeh.html

Grabosky, P. (2001). Computer crime: A criminological overview. Forum on Crime and Society, 1, 2-53.

Grabosky, P., Smith, R.G., Dempsey, G. (2001). Electronic theft: crimes of acquisition in cyperspace. Boston: Cambridge University Press.

Gross, H. (1971). Privacy and autonomy. In J. Pennock and J. Chapman. (Eds.). Privacy. pp. 169-182. New York: Atherton.

Gruber, A. (2007-2008). "Garbage pails and puppy dog tails: is that what Katz is made of?" 72 U.C. Davis L. Rev. 781.

Gubin, T. (2008). "Note: Warshak v. United States: the Katz for electronic communication." 23 Berkely Tech. L.J. 723.

Haas. T.C. (2001). Carnivore and the fourth amendment. 34 Conn. L. Rev. 261, 290.

Henderson, S. (2003-2004). "Nothing new under the sun: a technologically rational doctrine of fourth amendment search." 72 Geo. Wash. L.J. 805.

Hartzog, N. (2002). The "magic lantern" revealed: a report on the FBI's new "key logging" Trojan analysis of possible treament in dynamic legal landscape. 20 J. Marshall J. Computer and Info. L. 287.

Horn, K.A. (2002). Privacy versus protection: Exploring the boundaries of electronic surveillance in the internet age. 29 Fordham. Urb. L.J. 2223, 2274.

Huberman, Michael A and Mathew B. Miles (1994) "Data management and analysis Methods" in Denzin, Norman K. and Yvonna S. Lincoln (eds). Handbook of qualitative research. Thousands Oaks, CA: Sage.

Lessig, L. (1999). Code and other laws of cyberspace. New York: Basic Books.

Katz v. United States, 389 U.S. 347 (1967).

Kleinig, J. "Ethical perils of knowledge acquisition." Criminal Justice Ethics Vol. 28, No. 2, October 2009, 201-222

Kerr, O. (2002-2003). "Lifting the fog of internet surveillance: how a suppression remedy would change computer crime law." 54 Hasting L.J. 805.

Kerr, O. (2007) .http//www.volokh.com/archives/archive2007 02 04=2007 10/shtml#1170708253.

Kerr, D.M. (2000). Statement for the record on internet and data interception capabilities developed by FBI before the United States House of Representatives. Retrieved December 8, 2002, from http://www.fbi.gov/congress00/kerr0724000. htm

Krenn, P., Bem,D., Weissmann, A., (2008). "Mail Covers" (personal communications) USPIS. Washington DC, and New York City.

Kubic, T. (2001). Statement for the record before the house committee on the judiciary subcommittee on crime. Retrieved July 29, 2002, from Information Warfare Web sites: http://wwww. iwar.org.uk.ecoespionage/use-cybercrime/kubic_061201.htm

Kushner, H. (Ed.). (2002). Cyberterrorism in the 21st Century. Amer.ican Behavioral Scientist, 45.

Lukas.S (2001). "Current and future capabilities." Eds. A.Sofaer and S. Goodman, The tranational dimension of cyber crime and terrorism. Stanford University Press: Hoover Insitute.

Merl, S. R. (2001). Internet communication standards for the 21st century: International terrorism must force the U.S. to adopt "carnivore" and new electronic surveillance standard. 27 Brooklyn. J. Int'l.
245, 278.

Markoff, J. (2009). Worms infects millions of computers worldwide. New York Times, January 22. http//www.nytimes.com/2009/01/23/technology/internet/23worm.html.

Markoff.J. (2009). Vast Spy System loots computers in 103 countries. New York Times, March 28. http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=1

Marx, G. (1988). Undercover: Police surveillance. Berkeley: University California Press.

Marx, G.(1996). Privacy and technology. Teletronik, 1996.

Marx, G. (1998). An ethics for the new surveillance. Information society, 3, pp. 77-54.

Marx, G. (2001). Murky conceptual waters: public and the private Ethics and information technology, 3, 272-286.

Mulgan, T. (2001). The demand of consequentialism. New York: Oxford University Press.

Nance, A. (2002). Taking the fear out of electronic surveillance in the new age of terror. 70 UMKC. L. Rev. 751, 779.

Nardone v. United States, 308, U.S. 338 (1939).

Nisbet, R. (1971). The impact of technology on ethical decision making." In J.A. Douglas (Ed.). The technological threat. Englewood Cliffs: Prentice Hall.

Nissenbaum, H. (1998). Protecting privacy in the information age. Law and Philosophy. 17, 559-56.

O'Connell, Paul. (2002). Intellectual history of COMPSTAT. Ph.D. Dissertation, CUNY Graduate Center, Department of Criminal Justice

Olmstead v. United States, 277 U.S. 438 (1928)

Oyama, K. (2006) "Note: E-mail privacy after United States v. Councilman: legislative options for amending ECPA." 21 Berkely Tech. L.J. 499.

Peterson, M. (1994). Sources in crime analysis. Westport: Greenwood Press.

Pikowsky, R.A. (2002). An overview of the law of electronic surveillance post September 11, 2001. 94 Law Libr. J. 601, 619.

Pipkin, D. (2000). Information Security. Upper Saddle River: Prentice Hall.

Pollitt, M. (2001). Cyberterrorism---fact or fancy? Retrieved May 30, 2001from, http://cosc.georgetown.edu/~denning/infosec/pollitt/htm

Power, R. (2000). The tangled web. Indianapolis: Que.

Power, R. (2002). CSI/FBI computer crime and security survey. Computer Security: Issues and Trends, 7,1-17.

Redina, P. (2008). Personal communication. USPIS. Washington D.C.

Regan, P. (1995). Legistlating privacy. Chapel Hill: University of Carolina Press.

Rein, M.,and Schon, D, (1977). Problem setting in policy research. In C. Weiss (Ed.) Using Social Policy Research in Public Policy. Lexington, MA: DC, Heath.

Rosen, J. (2001). The unwanted gaze: The destruction of privacy in america.Vintage: New York, 2001.

Sager, I., Hamm, S., Gross, N., Carey, J. (2001, February 12). Cybercrime. Business Week Online. Retrieved June 7, 2003, from Web site: http://businessweek.com/2000/00_08/b3669001.htm?scriptFramed.

Salkever, A. (2001). A dark side to the FBI's Magic Lantern: http://www.businessweek.com/bw.daily/dnflash/nov2001/nf20011127 5011.htm

Sofaer, A., Goodman, S. (Eds.). (2001). The transnational dimension of cybercrime and terrorism. Stanford: Hoover Institution Press.

Smith v. Maryland, 442 U.S. 735 (1979)

Solove, D. (2002). Conceptualizing privacy. 90 Calif. L. Rev. 1087,1155.

Solove, D. (2003-2004). "Reconstructing electronic surveillance law." 72 Geo. Wash. L.J. 1264.

Source Watch, RESTORE Act (2007). http.//sourcewatch.org/index.php?title=Restore_Act(2007_FISA_bill)

Streeman, M. (2001). Cybercrime: liberty for security. Duke L. and Tech. Rev. 36

Strauss, Anselm and Juliet Corbin (1990). Basics of qualitative research: grounded theory procedures and techniques. Newbury Park. CA: Sage.

Sunstein, C. (2000). Republic.com. Princeton: Princeton U P.

Sutton, J.R. (2001). Law/society. Thousand Oaks: Sage.

Thomson, J. (1974). The right to privacy. Philosophy and Public Affairs, 4, 295-313.

United States v. , 567, F.2nd, 177 (9th Circ., 1978).

United States v, Councilman, 418 F. 3rd 67 (1st Circ. 2005) (en banc).

United States v. Jacobsen, 466 U.S. 109 (1984).

United States v. Herenandez, 313 F.3rd 1209 (9th Circ. 2002).

United States v, Leon Van Leewen, 387 U.S, U.S. 249 (1970).

United States v. Mark Stephen Forrester, 512 F.3d 500 (9th Circ. 2007)

United States v. Ramsey, 431 U.S. 606 (1977).

United States Department of State. (1996). The pattern of global terrorism. Washington, DC: Author.

U.S. Department of Justice. (2002). Searching and seizing and obtaining electronic evidence in criminal investigation.

United States Foreign Intelligence Surveillance Court of Review In Re Directives Pursuant to Section 105B of the Foreign Intelligence Act (2008).

National Criminal Justice Reference Services. Federal wiretap manual.

Van Den Haag, E. (1971). On privacy. In J. Pennock and J. Chapman.(Eds.). Privacy. (pp.149-169). New York: Atherton.

Wall, D. (Ed.). (2002). Crime and the internet. London: Routledge.

Weber, M. (1978). Economy and society: An outline of interpretive Sociology. Berkeley: University of California Press.

Westin, A. (1967). Privacy and freedom. New York: Atheneum.

Weinstein, W. (1971). The private and free: A conceptual inquiry. J. Chapman and J. Pennock. (Eds.). Privacy. (pp.27-56). New York: Atherton.

Winner, Langdon. (1977). Autonomous technology: Technics as a theme in political thought. Cambridge: MIT Press.

Williams, P. (2001). Organized crime, cybercrime: synergies, trends,Responses. Office of International Programs, U.S. Department of State. Retrieved June 7, 2003, from Information Warfare Website: http://www.iwar.org.uk/ecoespionage/resources/state/internet-crime.htm

Wilson. C. (2008) CRS REPORT FOR CONGRESS; botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for Congress. Congressional Research Service.

Yeats, J. (2002). "CALEA and RIPA: the U.S. and U.K. technologies in the wireless world." 12 Albany L.J. Sci and Technology Rev.

Yin, Robert K. (1984). Case study research: design and methods. Newbury Park, CA: Sage.

Yin, Robert K.(2003). Applications of case study research. Newbury Park, CA: Sage.

Young, M. (2001). What big eyes and ears you have!: a new regime for covert governmental surveillance. 70 Fordham. L. Rev. 1017, 1109