FREEDOM OF COMMUNICATION:
BREATHING SPACE IN THE MARKETPLACE OF IDEAS,
THE FIRST AMENDMENT IMPLICATIONS OF ELECTRONIC SURVEILLANCE

By

SUNNY SKYE HUGHES

A DISSERTATION PRESENTED TO THE GRADUATE SCHOOL
OF THE UNIVERSITY OF FLORIDA IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA

2008
© 2008 Sunny Skye Hughes
To my mom, Debbie.
ACKNOWLEDGMENTS

I conceived the idea for this dissertation while working with Bill Chamberlin at the University of Florida. I wish to thank him for his encouragement, advice, expertise and patience in reviewing the many incarnations and drafts of this document. I also wish to thank the members of my committee for their guidance and feedback: John Wright, Justin Brown and Charles Collier.

When I was a child, my mother was a cable splicer, and then lineman, for GTE. I said I would never grow up to work for the telephone company, but my early exposure to the telecommunications industry has had the most profound influence on my research. My mother is not alive to read this work, but I believe if she were, we would have much to debate. Thank you mom for always being my greatest fan and biggest critic.

Finally, I wish to acknowledge the patience of my friends and family as I worked to complete this monumental endeavor. Chris, your interest and endless hours discussing the finer points invigorated my academic pursuits. Forrest and Skyler, my beloved boys, I’m done with my dissertation now—yes, mom can play.
# TABLE OF CONTENTS

ACKNOWLEDGMENTS ...............................................................................................................4

ABSTRACT .....................................................................................................................................8

CHAPTER

1 INTRODUCTION ..................................................................................................................10

   Purpose ...................................................................................................................................13
   First Amendment Perspective .................................................................................................15
       Marketplace of Ideas .............................................................................................................16
       Key Values ..........................................................................................................................17
           Individual self fulfillment ...............................................................................................17
           Attainment of truth .........................................................................................................19
           Participation in decision-making .................................................................................19
           Balance between stability and change .........................................................................20
   National Security ....................................................................................................................23
   The Wall: The Fourth Amendment and Surveillance ............................................................25
   The Shifting Line: Liberty v. Security ....................................................................................33
   Chilling Effect ........................................................................................................................37
   Breathing Space ......................................................................................................................43
   Surveillance Societies (Dystopian and Utopian Visions) .......................................................45
   American Public Sentiment ....................................................................................................51
   Research Questions .................................................................................................................56
   Methodology ...........................................................................................................................57
   Definitions ..............................................................................................................................58
   Summary of Chapters .............................................................................................................61

2 LEGAL HISTORY OF DOMESTIC SURVEILLANCE BY US GOVERNMENT ............63

   The Black Chamber .................................................................................................................63
   The Radio Act of 1912 .............................................................................................................64
   The Radio Act of 1927 .............................................................................................................66
   The Communications Act 1934 ..............................................................................................67
   National Security Agency .......................................................................................................70
   Title III: Omnibus Crime Control and Safe Streets Act .......................................................73
   Church Committee ..................................................................................................................78
   Foreign Intelligence Surveillance Act ......................................................................................81
   Electronic Communications Privacy Act .............................................................................90
   CALEA ...................................................................................................................................92
   The Telecommunications Act of 1996 ..................................................................................97
   USA PATRIOT Act ...............................................................................................................98
   USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 .........................103
3 FIRST AND FOURTH AMENDMENT COURT DECISIONS ..........................................................115

The First Amendment Decisions ..........................................................................................115
  Schenck v. United States ....................................................................................................120
  Frohwerk v. United States ...............................................................................................122
  Debs v. United States .......................................................................................................124
  Abrams v. United States .................................................................................................126
  Gitlow v. New York .........................................................................................................132
  Whitney v. California .......................................................................................................136
  Bridges v. California .......................................................................................................140
  West Virginia State Board of Education v. Barnette .....................................................144
  Dennis v. United States .................................................................................................150
  Yates v. United States ....................................................................................................158
  Dombrowski v. Pfister ....................................................................................................166
  Lamont v. Postmaster General ........................................................................................168
  Ashton v. Kentucky .......................................................................................................170
  Stanley v. Georgia .........................................................................................................172
  Brandenburg v. Ohio .......................................................................................................173
  Gertz v. Welch ................................................................................................................175
  Breathing Space .............................................................................................................178
  Virginia v. Black ............................................................................................................179

Fourth Amendment Decisions ............................................................................................180
  Olmstead v. United States ..............................................................................................181
  Lopez v. United States ....................................................................................................191
  Griswold v. State of Connecticut ...................................................................................199
  Berger v. New York ........................................................................................................202
  Katz v. United States ......................................................................................................207
  United States v. United States District Court ................................................................213
  California Bankers Association v. Shultz .....................................................................220
  Zweibon v. Mitchell .......................................................................................................225

4 CONTEMPORARY ISSUES .................................................................................................228

  Technological Transition ...............................................................................................228
  The Terrorist Surveillance Program ..................................................................................233
  Contemporary Cases .......................................................................................................242
  Hepting v. AT&T .............................................................................................................243
    Count one ....................................................................................................................246
    Count two: ..................................................................................................................247
    Count three ..................................................................................................................249
    Count four ...................................................................................................................251
The United States government has monitored domestic telecommunications networks since the early twentieth century, but recent technological advancements have resulted in intelligence agencies having increased capabilities for monitoring content of communication, as well as the actual routing information for telephone calls. The monitoring of content through government surveillance is studied in this research from both a theoretical and legal perspective, tracing the history of United States surveillance, the development of the theory behind the marketplace of ideas, the evolution of domestic surveillance law and the potential impact a changing legal structure will have on citizen’s ability to express opinions without experiencing government censorship or punishment.

This research presents a First Amendment analysis of the changing legal structure of electronic surveillance, establishing a nexus between First Amendment rights to free speech and association and Fourth Amendment rights to privacy. This nexus is weighed against a historical balancing of concerns for protecting national security and concerns for protecting civil liberties. Contemporary court filings in response to government surveillance programs are evaluated to
explore the existence of a chilling effect on speech in the marketplace that might result from
government monitoring of citizen’s private communications.
CHAPTER 1
INTRODUCTION

Since September 11, 2001, the government has significantly modified laws governing electronic surveillance in the United States. The United States Administration and intelligence agencies have created new policies, such as the Terrorist Surveillance Program (hereinafter TSP), that governs electronic surveillance of citizen’s phone conversations. In many ways, these modifications have changed the understanding of how constitutional protections for Americans are interpreted. These modifications in some ways mimic the increased surveillance and monitoring engaged in by government agencies during past eras such as the communist scares during the McCarthy era. Contemporary policies have yielded a new round of suits filed by citizens and advocates who complain that not only their Fourth Amendment right to privacy, but also their First Amendment rights to free expression have been violated. Traditionally, judges have decided cases involving electronic surveillance on Fourth Amendment privacy grounds, but the new cases highlight a shifting balance between protections for civil liberties and national security. These new cases also make claims on grounds that there are First Amendment protections for telephone communications. Already, one judge has issued an opinion citing judicial precedent for the protection of free expression in private communications.

Although Fourth Amendment rights are the basis of most court decisions involving electronic surveillance, plaintiffs often invoke First Amendment protections for free speech, free religion and peaceable assembly. These First Amendment activities are protected not just nationally by the constitution, but internationally by human rights agreements. The Fourth Amendment’s guarantee of privacy, although not explicitly stated, insulates these rights by allowing citizens to develop political ideas and beliefs in private. This “breathing space” enables citizens to then dialogue in a public forum without government intervention and oversight.
Growing concerns over national security—specifically terrorism—may modify the understood legal balance between autonomous speech and national security. The purpose of this research is to examine the connection between Fourth Amendment protections for privacy and First Amendment protections for free speech and association by exploring the balance between citizen’s protections for civil liberties guarantees and the government’s need to protect national security.

Liberty, as it has developed in the United States, is experimental.1 Citizens must be able to discuss ideas freely, even if power holders consider those ideas subversive or dangerous.2 Fundamental to the marketplace of ideas model is the notion that citizens must feel free to express their ideas—the first step in this process is enjoying the privacy to develop these ideas.3 As John Stuart Mill theorized, reaching an informed political viewpoint that supports the democratic process may inevitably involve discussions of views that are not condoned or supported by citizens within the democracy.4 If this step in reaching a informed and well-thought out opinion is removed, then the resulting idea might not be as fully developed as possible had it undergone scrutiny and comparison to competing ideologies. In the past, ideologies such as socialism and communism have acted as foils to democracy, driving national

---

1 In 1947, the Hutchins Commission discussed this aspect of the marketplace of ideas. In its final report, the Commission concluded that,

Civilized society is a working system of ideas. It lives and changes by the consumption of ideas. Therefore, it must make sure that as many as possible of the ideas which its members have are available for its examination.


dialogue and clarifying American policies and ideals. If these political theories had been censored from the marketplace of national ideas, exploration of socialist and communist ideology might have been suppressed and eventually emerged as violent political dissent.

Today, terrorism—or more specifically, radical Islamic ideology and opposition to democracy, as well as opposition to government policies by American citizens—are the foil to American domestic and foreign policy. Given the parallels with past surveillance activities, the body of law developing around the above stated security concerns has the potential to threaten individual civil liberties, even as it protects national security interests of the country.

During the 21st century, the United States government has engaged in increasingly sophisticated surveillance of citizen’s communications. After September 11th, the United States declared a war on terrorism. One strategy in this war was to update electronic surveillance laws to defend the nation against this new threat to domestic security. How this initiative will affect citizen’s First Amendment rights has not yet been fully explored. Changes in laws that govern electronic surveillance could potentially affect the First Amendment rights of free speech, free assembly and the right to a free press. Expanded technological capabilities and increasingly sophisticated government controlled telecommunications networks and infrastructure also influence the laws that govern the electronic monitoring of citizen’s phone and Internet activities.

The Terrorist Surveillance Program could have a potential chilling effect on the First Amendment activities of United States citizens. This “chilling effect,” and its influence over the “breathing space” citizens need to develop well-reasoned political ideas, represents a changing paradigm in how government handles the interception of domestic telephone communications.

The modification of surveillance laws is a well-recognized threat to privacy, but the effect these changes will have on citizen’s ability to participate in the marketplace of ideas has yet to be
examined at a scholarly level. Increased government monitoring of telecommunication channels might act as a deterrent to citizens expressing unpopular ideas. If a person believes everything he or she says is monitored by the government, he or she may be less likely to voice unpopular opinions that contradict national policy. This potential stifling of the marketplace may have a negative effect on the democratic processes necessary to produce informed and engaged participants.

**Purpose**

Although the government has long monitored domestic telecommunication networks, the effect of this surveillance on citizen’s expression of subversive viewpoints has not yet been studied from a theoretical or legal perspective. This research traces the history of United States surveillance, the development of the theory behind the marketplace of ideas, the evolution of domestic surveillance law and the potential impact a changing legal structure will have on citizen’s ability to express opinions without experiencing government censorship or punishment.

This topic has become increasingly important, in part, due to developing technologies that facilitate the government’s monitoring of individual citizens without their knowledge. In the past, government agents would get a warrant or a court order to tap the phone line of a suspect. In the digital age, technology is in place that allows the same agents to intercept calls without the physical constraints of having to “bug” an individual phone line. Domestic calls are easily intercepted and filtered through sophisticated computer programs designed to detect “key words” and social connections between callers and known subversives.

The advances in the telecommunications infrastructure, coupled with the new terrorism crisis, mean current laws are outdated. The Bush administration acknowledged this when it disclosed the existence in 2005 of the Terrorist Surveillance Program, a secret domestic
wiretapping program that operated without warrants or judicial oversight. Neither the current administration nor scholars have been quick to address the implications an updated surveillance legal structure would have on citizen’s constitutional rights. In the literature, there are many legal analyses based on the Fourth Amendment right to privacy and how statutory changes would affect citizen’s rights to a secure home and secure correspondence. Although much of the literature and a few court opinions have acknowledged the First Amendment implications of these laws, there has yet to be a comprehensive analysis of this issue through legal and philosophical analysis.

A First Amendment analysis of the changing legal structure of electronic surveillance is timely and relevant. The Foreign Intelligence Surveillance Act, discussed in chapter two, was passed almost thirty years ago, at a time when most citizens had analog phone lines. In 2008, cell phones are common. The Internet is an everyday part of many citizens’ personal and professional life. These advances have created a wired society that is increasingly dependent upon these lines of communication. The current terrorism crisis has both amplified deficiencies in the statutory framework of FISA at the same time that it has created concerns among civil liberties experts who fear this perceived threat might result in limited constitutional protections. Threats to privacy from an unchecked surveillance program are easy to see, but the threats to the tangential free speech protections are subtle because they involve the citizen’s perception of the government’s intentions in monitoring their communications.

The First Amendment has a well-developed body of literature addressing free speech. Telecommunications research focuses heavily on regulations and technology. However, there has yet to be a thorough academic discussion of how these two areas relate to each other. By

---

examining the First Amendment implications of electronic surveillance, this research seeks to shed new light on the paradox between protecting national security and protecting individual rights to free speech and expression.

First Amendment Perspective

Several key First Amendment scholars have addressed concepts that apply to free expression in the context of electronic surveillance. Although these theories were not developed as directly applicable to surveillance, they are still theoretically sound principles for analyzing the impact government intervention can have in the sphere of private communications between citizens. Freedom in private communications supports the marketplace of ideas by enabling free expression. Freedom of the press is affected by the chilling effect of surveillance. Some of the forefathers believed that a free press would act as a fourth estate of government monitoring the actions of elected officials. John Locke, who was a great influence on America’s founders, crafted the social contract idea where the individual forfeits some of his rights for the betterment of society as a whole. Locke built on this idea with the concept that the press has an obligation to monitor official government actions in the interest of the individual, leading to a more informed electorate and a well-functioning democracy.

---


9 Id.
Marketplace of Ideas

A free exchange in the marketplace is necessary for truth to emerge over competing ideas. Public discourse is a necessary component in democracy. John Milton emphasized the necessity of public discourse in *Areopagitica* when he argued against government censorship through the Licensing Order of 1643. Milton wrote “let her [truth] and falsehood grapple; whoever knew Truth put to the worse in a free and open encounter,” advancing the idea that expression—as it informs the citizens-- should be free from prior restraint by the government. Milton was writing at the time of the Star Chamber when the King of England was seen as beyond criticism. The very act of speaking out against the government was a crime. Milton saw licensing as "the greatest displeasure and indignity to a free and knowing spirit that can be put upon him.”

Milton’s ideas in speaking out against this early form of censorship would be expanded in the writings of John Stuart Mill who explored freedom of expression in his book *On Liberty*. Mill wrote that anyone should be able to express anything, as long it did not harm other individuals. In his 1859 treatise, *On Liberty*, John Stuart Mill defended free speech as a necessary condition for intellectual and social progress. Mill went so far as to advocate letting
people air false statements and inferior theories so as not to silence elements of truth. Mill wrote that this approach promoted an open exchange of ideas and forced people to examine their beliefs through debate. This approach promoted a general understanding of one’s own position by allowing individuals to weigh the facts for themselves. Mill’s contributions to free speech theory primarily focused on printed materials. Other authors have applied these principles to the American experience of free expression within a legal framework.

**Key Values**

Thomas Emerson, in his 1963 *Yale Law Journal* article—and later in his 1970 book *The System of Freedom of Expression*, classified free expression into key values, or rather, reasons to protect the First Amendment. These include: 1) assuring individual self-fulfillment; 2) promoting discovery of truth; 3) the ability by all members of society to participate in decision making; and 4) the promotion of social stability through discourse. Each of these values can be abstractly applied to the protection of private discourse as a step towards engaging in free speech in the marketplace. Ensuring private discourse on unpopular viewpoints allows individuals to achieve self-fulfillment as individuals by bolstering their own ideas in the way imagined by Milton. Private discourse on unpopular ideas can also promote the discovery of truth.

**Individual self fulfillment**

Emerson said, “self-realization commences with development of the mind.” Conscious thought has no limits, as it is an individual process, with every man having a right to form and express his own beliefs and opinions. Emerson said, “expression is an integral part of the development of ideas, of mental exploration and of the affirmation of self.” The right to

---

17 Thomas I. Emerson, *supra* note 6 at 877.


19 Thomas I. Emerson, *supra* note 6 at 879.
expression is derived from the way that an individual is viewed as a societal member, not only in influencing culture, but also in being subject to societal influences and control.20

Given this role, the individual has a right of “access to knowledge,” so he can shape his views, as well as “communicate his needs, preferences and judgments.” Emerson said cutting off this “search for truth,” amounts to “despotic command,” where the individual is subject to arbitrary control. In exchange for being a cooperative member of society, the individual is rewarded with free expression.

Emerson viewed freedom of expression as “good in itself,” and essential to promoting other societal ends such as virtue, justice, and equality.

Hence the right to control individual expression, on the ground that it is judged to promote good or evil, justice or injustice, equality or inequality, is not, speaking generally, within the competence of the good society.

Emerson’s theory rested on the distinction between expression and action. Expression includes beliefs, opinions and communication of ideas, while action is synonymous with conduct. Society can seek to control conduct, but expression must enjoy a “specially protected position,” because it is the “fountainhead of all expression of the individual personality.” Emerson writes, “To cut off the flow at the source is to dry up the whole stream. Freedom at this point is essential to all other freedoms. Hence society must withhold its right of suppression until the stage of action is reached.” Furthermore, expression is seen as less injurious to social goals as it has less immediate consequences. The individual’s pursuit of self fulfillment, as well as the balance between security and liberty, discussed in chapter one, is at jeopardy when expression is restricted for political goals:

20 Id. at 880.
the power of society and the state over the individual is so pervasive, and construction of doctrines, institutions and administrative practices to limit this power so difficult, that only by drawing such a protective line between expression and action is it possible to strike a safe balance between authority and freedom.\textsuperscript{21}

**Attainment of truth**

Emerson believed that human judgment is frail and by nature, incomplete, therefore freedom of expression is essential to in allowing members of a society to “make full use of different minds to sift the true from the false.”\textsuperscript{22} Suppression of this expression impedes the creation of new ideas.

Many of the most widely acknowledged truths have turned out to be erroneous. Many of the most significant advances in human knowledge—from Copernicus to Einstein—have resulted from challenging hitherto unquestioned assumptions. No opinion can be immune from challenge.\textsuperscript{23}

Even opinions that turn out to be false promote discussion and serve the “vital social purpose,” of compelling the “rethinking and retesting of the accepted opinion.” Emerson said that “social judgment is made up of individual judgments,” and therefore is dependent upon the competition of ideas. In the end, the only way that an individual, and society as a whole, can attain truth is to have open dialogue and discourse on ideas, free from government control.

**Participation in decision-making**

Open discussion amongst members of the community also promotes decision making.\textsuperscript{24} This discussion, when restricted to only the “elite” deemed worth of expression, denies individual participation by those who may have valuable opinions or facts to contribute to the community discussion. Although this participation is vital in many community affairs such as

\textsuperscript{21} Id.

\textsuperscript{22} Id.

\textsuperscript{23} Id.

\textsuperscript{24} Id. at 882.
culture and planning, it is vital in the political process because “the state has a special incentive
to repress opposition and often wields a more effective power of suppression.” Emerson also said
that “Freedom of expression in the political realm is usually a necessary condition for securing
freedom elsewhere.” Political freedom of expression also allows citizens to communicate their
“attitudes, needs and wishes” to a responsive government. Emerson emphasized that this
freedom of expression is not just “politically useful,” but “indispensable to the operation of a
democratic form of government.” This communication between citizens and their government is
what promotes good representative democracy, with citizens influencing and participating in
democratic governance.

Balance between stability and change

The final key value identified by Emerson is the balance between stability and change,
with “open discussion” as a means for “achieving a more adaptable and at the same time more
stable community.” Emerson said that suppression of discussion inhibits rational discussion,
prevents social change, minimizes the development of new ideas, and “conceals the real
problems confronting a society.” Without free expression, ideas are driven underground, and
“makes resort to force more likely.” Emerson said that free expression leads society to “greater
cohesion.”

The principle of political legitimation, however, is more broadly fundamental. It asserts
that persons who have had full freedom to state their position and to persuade others to
adopt it will, when the decision goes against them, be more ready to accept the common
judgment. They will recognize that they have been treated fairly, in accordance with
rational rules for social living. They will feel that they have done all within their power,
and will understand that the only remaining alternative is to abandon the ground rules
altogether through resort to force, a course of action upon which most individuals in a

\[\text{Id. at 884.}\]
healthy society are unwilling to embark. In many circumstances, they will retain the opportunity to try again and will hope in the end to persuade a majority to their position.26 Emerson’s theory was that “change is inevitable,” and “freedom of expression offers possibilities for rational, orderly adjustment.”27 Emerson said that a system of free expression must recognize the “distinction between expression and action,” with expression being “free and unrestrained.”28 Emerson concluded by saying the “natural balance of forces in society today tends to be weighted against individual expression,” and this necessitates a “positive approach, in which law and judicial institutions play a leading role.”

Alexander Meiklejohn also understood the purpose of the First Amendment as a guarantee of individual participation in the political decision making process.29 He analogized that free speech was a town meeting, allowing citizens to come together, proclaim opinions and beliefs, and reach a consensus based on lively debate.30 Freedom of speech does not indicate a “free-for-all” where “every individual has an unalienable right to speak whenever, wherever he chooses,” but rather “it is a group of free and equal men, cooperating in a common enterprise, and using for that enterprise responsible and regulated discussion.”31 Meiklejohn emphasized that in self government, it is not that “everyone shall speak, but that everything worth saying shall be

26 Id. at 885.
27 Id. at 886.
28 Id. at 955.
30 MEIKLEJOHN, POLITICAL FREEDOM, supra note 29 at 23-24.
31 Id.
said.” Even with this restraint, participants in self-governing democracies must meet ideas “with their eyes open. Meiklejohn said, “To be afraid of ideas, any idea, is to be unfit for selfgovernment. Any such suppression of ideas about the common good, the First Amendment condemns with its absolute disapproval.”

The guarantee given by the First Amendment is not, then, assured to all speaking. It is assured only to speech which bears, directly or indirectly, upon issues with which voters have to deal—only, therefore to the consideration of matters of public interest. Private speech, or private interest in speech, on the other hand, has no claim whatever to the protection of the First Amendment.

Meiklejohn reconciled the competing interests of society and the individual by making five observations on the relationship between government and citizens: 1) the public interest is made up of “individual desires and intentions,” and must combine all concerns; 2) given that human interests are in “constant conflict with one another, they cannot all be realized.” The common good is not a collection of concerns, and often one interest is sacrificed for another; 3) government judgments should be based upon “general principles” such as “unity, justice, tranquility, defense, welfare, equality, liberty.” This might require the sacrifice of individual rights; 4) the government must balance protection of collective and individual rights; 5) the constitution shows no preference in the balancing of collective and individual rights, but rather “the American Way of Life is free because it is what we Americans freely choose—from time to time—that it shall be.”

---

32 Id. at 24.
33 Id. at 27.
34 Id. at 94.
35 Id. at 96-98.
National Security

Harold Lasswell, in his 1950 book *National Security and Individual Freedom*, developed the communication theory of interacting systems, said that individuals should have an increased role in controlling the governing process. This individual control is a response to what Lasswell described as a “central nervous system” controlling the country’s communications. Lasswell said that civilian supremacy is a “characteristic of democratic government” evident in the intentions of the forefathers to protect individual freedom against “arbitrary official action.”

Lasswell said that the First Amendment is most the most essential protection of the political process because it guarantees free expression. During Lasswell’s time, courts used the “clear and present danger” test to evaluate First Amendment protections for speech tempered by national security concerns. Lasswell said that the application of this test required an “independent estimate of the necessities of the situation.” This estimate is only possible if the courts have all the information about the programs may be limiting constitutional rights. Lasswell urged continued judicial review of such information through the “National Security Council” in order to limit security threats.

---

36 HAROLD LASSWELL, NATIONAL SECURITY AND INDIVIDUAL FREEDOM 141-42 (1950).
37 Id.
38 Id. at 65.
39 Id. at 141-42.
41 LASSWELL, supra note 36, at 142.
42 Id.
interpretation would limit the abuse of power by a garrison state.\textsuperscript{44} Lasswell said that when intelligence agencies are allowed to operate beyond judicial review, civil liberties may be threatened by political agendas.\textsuperscript{45}

Lasswell introduced four principles to generally govern national security programs\textsuperscript{46}:

I. Is there a threat to the principle of civilian supremacy in the U.S. system of government?

II. Does the policy involve a threat to freedom of information and disclosure of government activities?

III. Is there danger to the civil liberties of the individual?

IV. Does the policy violate the principle of a free—as opposed to a controlled—economy?

Lasswell said that an affirmative answer to any of these questions triggers a “potential loss of freedom,” which can be avoided or reduced by changing the national security program in question. Lasswell said reducing the reach of government security programs might preserve the American goal of individual dignity.\textsuperscript{47}

\textsuperscript{401 et seq. (2000)). Later in 1949, as part of the Reorganization Plan, the Council was placed in the Executive Office of the President. According to the Whitehouse:

The National Security Council is chaired by the President. Its regular attendees (both statutory and non-statutory) are the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, and the Assistant to the President for National Security Affairs. The Chairman of the Joint Chiefs of Staff is the statutory military advisor to the Council, and the Director of National Intelligence is the intelligence advisor. The Chief of Staff to the President, Counsel to the President, and the Assistant to the President for Economic Policy are invited to attend any NSC meeting. The Attorney General and the Director of the Office of Management and Budget are invited to attend meetings pertaining to their responsibilities. The heads of other executive departments and agencies, as well as other senior officials, are invited to attend meetings of the NSC when appropriate. The National Security Council is the President’s principal forum for considering national security and foreign policy matters with his senior national security advisors and cabinet officials. Since its inception under President Truman, the function of the Council has been to advise and assist the President on national security and foreign policies. The Council also serves as the President’s principal arm for coordinating these policies among various government agencies. See National Security Council, http://www.whitehouse.gov/nsc/.

\textsuperscript{44} Id. at 143.

\textsuperscript{45} Id.

\textsuperscript{46} Id. at 57.

\textsuperscript{47} Id.
The Wall: The Fourth Amendment and Surveillance

The “Wall” between foreign intelligence gathering and criminal law enforcement is a common theme in the literature on the topic of FISA surveillance. Richard Seamon and William Gardner discussed the wall in their 2005 *Harvard Journal of Law and Public Policy* article, “The PATRIOT Act and the Wall Between Foreign Intelligence and Law Enforcement.” Attorney General Janet Reno adopted procedures requiring Justice Department officials to construct “a wall” to prevent “sloppy” compliance with the primary purpose test in 1995. This wall mainly consisted of three provisions including

1. prohibiting the DOJ’s Criminal Division\(^{50}\) from giving the Federal Bureau of Investigations (FBI) advice that would “result in either the fact or appearance of the Criminal Division’s directing or controlling foreign intelligence or foreign counterintelligence,

2. requiring that the FBI and the Justice Department’s Office of Intelligence Policy and Review (OIPR) notify the criminal division of any FBI surveillance investigations that yielded evidence reasonably indicating that a “significant federal crime has been, is being, or may be committed,” and

3. requiring that the OIPR act as a gatekeeper controlling information flow between the FBI and the Criminal Division regarding intelligence or potential prosecutions.\(^{51}\)

---


\(^{49}\) Id. at 367.

\(^{50}\) According to the website for the Department of Justice Criminal Division,

> The Criminal Division develops, enforces, and supervises the application of all federal criminal laws except those specifically assigned to other divisions. The Division, and the 93 U.S. Attorneys have the responsibility for overseeing criminal matters under the more than 900 statutes as well as certain civil litigation. Criminal Division attorneys prosecute many nationally significant cases. In addition to its direct litigation responsibilities, the Division formulates and implements criminal enforcement policy and provides advice and assistance.

The division also advises the Attorney General, Congress, the Office of Management Budget and the White House on matters of criminal law, providing legal advice and assistance to federal prosecutors and investigative agencies (such as the FBI). U.S. Department of Justice, Criminal Division, [http://www.usdoj.gov/criminal/](http://www.usdoj.gov/criminal/) (last visited June 22, 2008).

\(^{51}\) Seamon & Gardner, *supra* note 48 at 368-71.
Seamon and Gardner suggested that the 2001 PATRIOT Act changed the nature of the FISA wall by removing the original requirement that surveillance be conducted for the “primary purpose” of obtaining foreign intelligence.\(^{52}\) Post PATRIOT, the wall was eroded by the requirement that foreign intelligence gathering need only be a “significant purpose” in the order seeking a FISA warrant.\(^{53}\) For example, in a criminal investigation into drug trafficking, warrant requests would normally be made under Title III of the federal electronic surveillance statutes, discussed in chapter two. With the change in purpose discussed above, federal agents investigating drug traffickers who were also suspected of terrorism, could apply for a less restrictive FISA warrant. The authors conclude by calling for Congress to amend FISA and clarify the wall between foreign intelligence gathering and criminal law enforcement investigations.\(^{54}\)

Senator Orrin Hatch (R-Utah) clarified the change in the primary purpose test when he spoke before the Senate Judiciary Committee in 2002. Hatch said Congress intended to enable the gathering of foreign intelligence as a “significant purpose,” even when the primary purpose of the intelligence was a criminal investigation.\(^{55}\) The primary purpose of the surveillance would be foreign intelligence if intelligence investigators managed the surveillance.\(^{56}\) The primary

---

\(^{52}\) Id. at 376.

\(^{53}\) Id. at 376-77.


\(^{55}\) Id.
purpose would be a criminal investigation if criminal investigators managed the surveillance.\textsuperscript{57} If the primary purpose is a criminal investigation, then the government must honor Title III’s stricter requirements for surveillance so the search would not violate a domestic target’s Fourth Amendment right against unreasonable search and seizure.\textsuperscript{58} Title III and FISA both require the government to establish probable cause for the court to issue an order for the use of electronic surveillance.\textsuperscript{59} Title III requires the court to find probable cause on the “basis of the facts submitted” that an individual is, has or is about to commit, a crime. FISA requires the court to find probable cause "on the basis of the facts submitted that the individual is a foreign power or agent of a foreign power. Whereas, Title III requires facts substantiating a crime, FISA requires only an association with a foreign power.

Given the recency of the disclosure of the Terrorist Surveillance program, few authors other than journalists have had an opportunity to study the issue. Barbara Bergman offered a notable exception in her February 2006 column for \textit{Champion}, a magazine that informs criminal defense lawyers of developments in search and seizure laws. Bergman said that Congress never gave the executive branch permission to conduct electronic surveillance without wiretaps, even if it was informed in a limited manner.\textsuperscript{60} Bergman’s comparison looked at the Administration’s claim that Congress was informed of the surveillance program, therefore it cannot be found illegal. She likened Bush’s actions to one of her clients basing a defense on the fact he told his

\textsuperscript{57} \textit{Id.}

\textsuperscript{58} \textit{Id.}


friends he was going to commit a crime. Bergman cited the Supreme Court’s ruling in *U.S. v. United States District court* to say that judicial approval is required, in addition to informing Congress. Bergman said that Congress passed FISA, discussed in chapter two, as a means to monitor domestic individuals who might be working for foreign powers. She did not endorse FISA, but said that it has been severely crippled by the PATRIOT Act—specifically Congress’ modification to the primary purpose requirement for foreign intelligence. Bergman concluded by calling for Congressional hearings to investigate the change and its effect on American civil liberties.

Bergman’s piece is representative of existing information on the latest FISA developments, but most of the literature available does not focus specifically on the President’s terrorist surveillance program. Rather, the literature available discusses general problems with electronic surveillance. Literature in this area focuses on three major themes: the legislative history of FISA, “the wall” established to separate foreign intelligence and law enforcement activities across government agencies, and the need to reform current surveillance provisions. An undercurrent in all of the literature reviewed is the need for balance between security and liberty.

J. Christopher Champion, in his 2005 *Vanderbilt Law Review* article, analyzed FISA’s legislative history. Champion also reviewed the Foreign Intelligence Surveillance Court’s

---

61 *Id.* The *Champion* is a magazine published by the National Association of Criminal Defense Lawyers that covers issues of concern to criminal defense lawyers and the “latest developments in search and seizure laws.”

62 United States v. U.S. District Court (“Keith”), 407 U.S. 297, 323-24 (1972). (holding that “prior judicial approval is required for the type of domestic surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.”)

63 Bergman, *supra* note 60.

64 Bergman, *supra* note 60. For further discussion of primary purpose test, see *infra* pp. 29 & 99.

65 Bergman, *supra* note 60.
(FISC) 2002 role in reinterpreting FISA based on the PATRIOT Act’s 2001 amendment of the primary purpose test. Pre-PATRIOT, FISA warrants only allowed collection of information related to “foreign intelligence crimes.” In 2002, the FISC emphasized the separation of foreign intelligence and criminal law enforcement investigations, despite language in the PATRIOT Act aimed to dissolve this “wall” between the two distinct surveillance purposes.

The court, in denying the Department of Justice’s request to involve criminal law enforcement in FISA surveillance, relied on the 1980 case of United States v. Truong Dinh Hung. In this case, the Fourth Circuit of the U.S. Court of Appeals upheld the warrantless surveillance of agents of foreign powers, including U.S. citizens when they are acting as foreign agents as long as the primary purpose of the surveillance was foreign intelligence. The FISC of review overturned the 2002 FISC ruling reasoning that the Truong case misinterpreted the minimization procedures outlined in FISA. Minimization is a term that refers to the principle that intelligence agencies should minimize the “collection, retention, and dissemination of information” on U.S. citizens

---

66 J. Christopher Champion, The Revamped FISA: Striking A Better Balance Between The Government's Need To Protect Itself And The 4th Amendment, 58 VAND. L. REV. 1671 (2005). See also Designation of Judges, 50 U.S.C. § 1803 (2000). The United States Foreign Intelligence Surveillance Court (FISC), a federal court authorized by FISA, reviews and grants applications for electronic surveillance warrants by federal agencies. The court originally had seven federal district judges, but the PATRIOT Act changed that number to eleven requiring at least three of the judges to be within twenty miles of Washington, D.C. The chief justice of the United States Supreme Court appoints the judges. The FISC hearings are closed to the public and court records are classified. The FISC of review can grant, deny or modify requests for warrants. The federal government is the only party in the court’s proceedings, and denials for orders are appealed to the United States Foreign Intelligence Surveillance Court of Review.

67 Id.


69 Id.

who are subjects of FISA authorized wiretaps.\textsuperscript{71} One aspect of minimization is an “information-screening wall” that allows information to be passed to law enforcement officials only when relevant evidence is discovered.

Champion said the courts need to strike a better balance between FISA and the Fourth Amendment.\textsuperscript{72} Champion’s called for a better balance reflecting the complex nature of the issue and a possible need to reevaluate the line between security and privacy in light of the changes made by the PATRIOT Act and the FISC’s 2002 ruling.\textsuperscript{73} The FISC of review said a “wall” could not necessarily separate criminal law enforcement and foreign intelligence activities since investigations often involved both activities.\textsuperscript{74} Essentially, the FISC ruled that FISA was never meant to be limited to foreign intelligence collection.\textsuperscript{75} This 2002 FISC ruling further eroded the wall between foreign intelligence and criminal law enforcement.

\textsuperscript{71} Executive Order 12333, issued in 1981 by President Reagan, required that intelligence agencies “use the least intrusive collection techniques feasible within the United States or directed against U.S. persons abroad.” Exec. Order No. 12333, 3 C.F.R. 200 (1981 Comp.).

\textsuperscript{72} Champion, \textit{supra} note 66 at 1703.

\textsuperscript{73} See also David. S. Jonas, \textit{The Foreign Intelligence Surveillance Act Through The Lens Of The 9/11commission Report: The Wisdom Of The Patriot Act Amendments And The Decision Of the Foreign Intelligence Surveillance Court Of Review}, 27 N.C. CENT. L.J. 95 (2005). Jonas takes an approach similar to Champion in his article on the post-PATRIOT-Act FISA; however his remedies and conclusions differ greatly. Jonas’ article reviews FISA legislative history and amendments. He looks at the implications of terrorism on domestic surveillance before concluding that the PATRIOT Act’s amendments to FISA were necessary given the circumstances surrounding 9/11 and national sentiment following the attacks. He suggests that instead of limiting the tools needed to fight the War on Terrorism, there should be harsher penalties for those in the executive branch who abuse power. Jonas bases his recommendations on the idea that terrorists pose a great threat to U.S. national security. Jonas suggests that the preservation of the United States democratic system is dependent upon defending against the terrorist threat. He states “insecurity threatens liberty.” The author discusses the national security pendulum that shifts constantly between individual rights and national security. Jonas says that the 9/11 Commission has suggested that “now is the time for the pendulum to swing towards national security.” He says the key to realizing that shift is effective intelligence, which does not punish cooperation between agencies for the purposes of national security.

\textsuperscript{74} \textit{In re} Sealed Case No. 02-001, 310 F.3d 717 (U.S. Foreign Intell. Surveil. Ct. 2002), \textit{available at} http://www.cnss.org/FISCR_opinion.pdf.

\textsuperscript{75} The primary purpose test developed as a Fourth Amendment restriction on warrantless electronic surveillance. After the 1967 \textit{Katz} ruling, discussed in chapter three, electronic surveillance conducted by the government was viewed by the Supreme Court as search and seizure that activated Fourth Amendment protections. A line of case law developed from this ruling indicating warrantless electronic surveillance was legal if conducted for the primary purpose of obtaining foreign intelligence information. In \textit{United States v. Brown}, 484 F.2d 418 (1973), the Third
Heath H. Galloway, in his 2002 Washington and Lee Law Review article, saw the erosion of the FISA wall as the latest in a series of attacks on American’s privacy. He said the attacks are more common when the government has increased power. Galloway said changes to FISA are not necessarily evil, but that “evil has made them a necessity.” The September 11th attacks reinforced the idea of “terrorism” as an “evil” that required a reevaluation of existing statutes related to electronic surveillance.

Jennifer M Hannigan used a 2004 Houston Law Review Comment to boldly state “toying with civil rights post-9/11 may ironically help terrorists accomplish their goals by impacting the American ideals of freedom and liberty.” She discussed the cycle of U.S. civil liberties violations by analyzing Supreme Court Justice William J. Brennan’s factors for infringement of

Circuit of the U.S. Court of Appeals found that warrantless wiretaps were constitutional because they were authorized by the Attorney General “for the purpose of gathering foreign intelligence.” In United States v. Butenko, 318 F. Supp. 66 (D.N.J. 1970), aff’d, United States v. Butenko, 494 F.2d 593 (3d Cir. 1974), the U.S. Court of Appeals for the Third Circuit found that the Fourth Amendment did not require a warrant for wiretapping when the primary purpose of the surveillance was gathering foreign intelligence. In United States v. Truong, 629 F.2d 908 (4th Cir. 1980), the Fourth Circuit suppressed evidence under what would be frequently cited as the first use of the “primary purpose test.”

Heath Heath H. Galloway, Don’t Forget What We’re Fighting For: Will the Fourth Amendment Be A Casualty of the War on Terror, 59 WASH. & LEE L. REV. 921 (2002). See also Robert N. Davis, Striking the Balance: National Security vs. Civil Liberties, 29 BROOK. J. INT’L L. 175 (2003). Davis provided a look at the history on intelligence gathering since the 1947 National Security Act, outlining the national defense strategy from 1947-2003. He discusses how the PATRIOT Act amended FISA and offers recommendations to remedy the erosion of “the Wall.” Davis, in his conclusion, focused on the National Emergencies Act of 1976, Pub. L. No. 94-412, 90 Stat. 1255 (1976) (codified as amended at 50 U.S.C. §§1601-1651) (2000), which gave Congress a statutory basis for monitoring the President’s declaration of a national emergency. He said President Bush used the terrorist attacks as a justification to declare a state of national emergency. This state of emergency governs the War on Terrorism, where the U.S. seeks to “destroy terrorists and those who support them wherever they may be.” Davis said the country has come “full circle.” Whereas the Church Committee (1975-1976) was motivated to constrain intelligence activities based on national events, terrorism might be a cause to “untie the hands of the intelligence community.” Davis said that the balance between national security and the Fourth Amendment is at the center of the issue. Davis added that civil liberty protection relies upon the survival of the nation—if a nation is not secure, civil liberties are threatened. He used this reasoning to establish the idea that the nation must be preserved in order to preserve freedom.

Galloway, supra note 76.

Id. at 974.

civil rights during a time of crisis. Under this model: 1) the crisis creates a national fervor, 2) security risks are exaggerated and 3) the perceived risks result in a forfeiture of civil liberties until the risk subsides. Hannigan said decision makers’ difficulties in identifying true security risks, amongst perceived risks that might never manifest to true security threats, perpetuate the cycle. Hannigan said the real threat of terrorism is that it provokes “democratic regimes to embrace and employ authoritarian measures.” She concluded by suggesting that the nature of the 9/11 attacks have resulted in a new crisis with no definable end.

The existing literature not only explores FISA, the PATRIOT Act and related statutes, but also includes review of possible changes that might be made to current intelligence practices in order to update methods to protect American’s constitutional rights and the country’s interests. In discussing the “wall” between law enforcement and foreign intelligence, the authors discussed above take different approaches regarding the best remedy. What emerges as a common lens is the shifting line between security and liberty. Whereas some authors, such as Galloway in the Washington and Lee Law Review, see the erosion of the wall between foreign and domestic surveillance as necessary to preserve national security, others, such as Hannigan in the Houston Law Review, see it as a threat to liberty. The War on Terrorism is one reason for the erosion of the wall between foreign intelligence and criminal law enforcement, but it is not the only factor involved in the changing nature of electronic surveillance. Telecommunications technology is changing at a rapid pace. Legislators struggle to keep laws current with technological

---

80 Id. at 1375. See William J. Brennan, Jr., The Quest to Develop a Jurisprudence of Civil Liberties in Times of Security Crises, Speech at the Law School of Hebrew University, Jerusalem, Israel, at 1 (Dec. 22, 1987).

81 Hannigan, supra note 79 at 1375.

82 Id. at 1390.

83 Id. at 1405.
advancements and new threats to security. The convergence of a growing terrorist threat and a rapidly changing telecommunications industry are at the root of the paradigm shift that is forcing the reexamination of the line between national security and privacy. The shifting balance between these two concerns has a direct impact on First Amendment protections for American citizen’s free speech.

**The Shifting Line: Liberty v. Security**

Liberty is a central theme in the founding principles of the United States of America.84 One interpretation of “liberty” is freedom from the arbitrary exercise of authority.85 This has been called a “negative liberty,” because the protection is not explicitly stated in the Constitution. Liberty—from government actions that interfere with a person’s ability to do what they choose—is then derived from the Fifth Amendment’s protection from self incrimination, and the Fourteenth Amendment’s due process and equal protection clauses86 As in John Locke’s social contract theory, citizens frequently—and willingly—accept intrusions on their “negative liberty”

---

84“‘We hold these truths to be self-evident, that all men are created equal, that they are endowed by their creator with certain unalienable rights, that among these are life, liberty and the pursuit of happiness.’ **THE DECLARATION OF INDEPENDENCE** (U.S. 1776).

“We the people of the United States, in order to form a more perfect union, establish justice, insure domestic tranquility, provide for the common defence, promote the general welfare, and secure the blessings of liberty to ourselves and our posterity, do ordain and establish this Constitution for the United States of America.” **U.S. CONST.** prmb.

85 **BLACK’S LAW DICTIONARY** 930 (7th ed. 1999). See also **U.S. CONST.** amend. V, which says no one “shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law” See also **U.S. C CONST.** amend. XIV, which says the state should not deprive “any person of life, liberty, or property, without due process of law.” See also **AM. JUR. 2D** Const. Law §562 (2008) (citing Ingraham v. Wright, 430 U.S. 651 (1977)).

86 **ISAIAH BERLIN, LIBERTY** (2002).
as a necessity of government trying to protect the “positive liberties” of freedom of the mind, freedom of action, choice and equal protection.87

Citizen concerns over national security influence how the concept of liberty is interpreted and applied. For example, the National Security Strategy of the United States—the official policy of the Executive Branch in protecting national security—defines liberty as the use of power to maintain the integrity of the state.88 This relationship between liberty and national security is very different than the one between liberty and personal security. This is reflected by John Jay’s assertion in the Federalists Papers

Nothing is more certain than the indispensable necessity of Government, and it is equally undeniable, that whenever and however it is instituted, the people must cede to it some of their natural rights, in order to vest it with requisite powers.89

This assertion shows the constitutional framer’s reliance on the ideas of British philosophers, such as John Locke, in recognizing the willingness of citizens to cede protection of personal liberty for the purpose of protecting national security. This voluntary forfeiture of liberty reflects the “line” that marks the balance between the two realms of security.90 British philosophers such as Locke and Hobbes defined this line as the boundary between the zones of personal liberty and government authority.91

---

87 That to secure these rights, Governments are instituted among Men, deriving their just powers from the consent of the governed. U.S. CONST. pmbl. See also JOHN LOCKE, TWO TREATISES OF GOVERNMENT (1689), available at http://socserv2.mcmaster.ca/~econ/ugcm/3ll3/locke/government.pdf.


89 THE FEDERALIST NO. 2 (John Jay).

90 British philosophers such as Locke and Hobbes defines this line as the boundary between the zones of personal liberty and government authority. See generally HOBBES AND BRAMHALL ON LIBERTY AND NECESSITY (Vere Chappell ed., Cambridge U. Press 1999).

91 Id.
Former NSA Director Michael Hayden mentioned the “line” between liberty and security in his testimony before the Senate Select Committee on Intelligence in 2002. Hayden said “free people must draw the line between their liberty and their security.” Hayden suggested the September 11th attacks would drive the nation more toward security. He then challenged the NSA to keep America free through a renewed feeling of safety. Hayden said the “line drawing” affects the NSA’s activities including surveillance standards, data collection and dissemination. Hayden suggested the attacks were cause for reevaluation of where the line was drawn. After the attacks of September 11th, the theme of protecting “national security” became commonplace in political rhetoric, media accounts and public sentiment.

---


94 *Id.*

95 *Id.*

96 *Id.*

97 *Id.* Specifically, the NSA Director said “We need to get it right.”

In December of 2005, The Terrorist Surveillance Program drew national attention to the line between liberty and security.\(^9\) Just days after the disclosure of the Terrorist Surveillance Program, Attorney General Gonzales, in a press conference, explained how the National Security Agency managed its mission to protect Americans in the “spectrum” between liberty and security:

Across the board, there is a judgment that we all have to make -- and I made this speech a day or two after 9/11 to the NSA workforce -- I said, free peoples always have to judge where they want to be on that spectrum between security and liberty; that there will be great pressures on us after those attacks to move our national banner down in the direction of security. What I said to the NSA workforce is, our job is to keep Americans free by making Americans feel safe again. That's been the mission of the National Security Agency since the day after the attack, is when I talked -- two days after the attack is when I said that to the workforce.\(^{10}\)

National security concerns influence how the line between security and liberty is drawn. Laws such as FISA have been passed to specifically protect the civil liberty interests of American citizens. Furthermore, changes in the telecommunications industry have resulted in technological advancements enabling carriers to better assist the government in capturing and filtering private communications. Gone are the days of government agents requesting copies of telegrams; now, sophisticated computer software can filter comprehensive databases looking for suspicious patterns or key words.

---

\(^9\) Risen & Lichtblau, supra note 5. In December of 2005, Congress met to negotiate extending the powers of the USA PATRIOT Act of 2001, a statute largely concerned with demolishing the historical wall between intelligence and law enforcement.

Chilling Effect

The chilling effect was first mentioned in a 1951 *Vanderbilt Law Review* article by Paul Freund exploring a double standard in the judicial treatment of civil liberties.101 Freund reasoned that a judicial rule against vagueness or over breadth should depend on the moral quality of the conduct, so as to not “chill” constitutionally protected conduct that might have “genuine social utility.” This differentiation of activities based on morality protects the public interest in freedom of expression by providing for a rational exploration of political ideas.102 Freund argued that the “chilling” of constitutional protections can be just as bad as “prohibiting” them in the cases of monitoring subversive phone conversations.103

When government intervenes in the marketplace of ideas, regulations can have a “chilling effect” on free speech and open dialogue.104 Frederick Schauer, in a 1978 article for the *Boston Law Review*, wrote that the chilling effect doctrine was a combination of two legal principles. First, the legal process is uncertain because it involves “people-made rules” and it is difficult to have a high degree of confidence in predicting outcomes.105 Second, the legal system is wrought with errors, which, in the context of free speech, poses greater comparative harm to an individual and the legal process.106 Schauer suggested that the government imposition of restrictive laws of

---

102 *Id.* at 540, 549.
105 *Id.* at 687.
106 *Id.* at 687-88.
free expression does not create “benign” deterrence, but “invidious” deterrence of protected activities.  

The very essence of a chilling effect is an act of deterrence. While one would normally say that people are deterred, it seems proper to speak of an activity as being chilled. The two concepts go hand in hand, of course, in that an activity is chilled if people are deterred from participating in that activity. Although an individual's decision not to engage in certain behavior may be influenced by a wide range of stimuli, in law the acknowledged basis of deterrence is the fear of punishment—be it by fine, imprisonment, imposition of civil liability, or deprivation of governmental benefit.

Schauer said that the chilling effect is a “subset of the inhibitory effect created by any regulatory enactment and creates no independent constitutional difficulties.” The chilling effect is implicated when any Constitutional safeguard is “unduly discouraged,” including activities protected by the First Amendment. First Amendment protections provide an “affirmative value” protecting a right to speak. Schauer said that this affirmative right has the positive social value of promoting the public exchange of ideas and information. Schauer said that the government must evaluate interference in the “positively advantageous” sphere of free speech, as it is a constitutionally protected realm.

Schauer said that the chilling effect is not dependent upon altering specific behaviors, rather it is based on the “comparative nature of the errors that are bound to occur,” in regulating activities that are bound up with constitutionally protected activities. This comparative effect—

---

107 Id. at 690. Historian Howard Zinn mentioned a “chill” on free speech in the chapter of his book on American ideology. In discussing the First Amendment, he envisioned a scenario where “all of the restrictions on freedom of speech” are suddenly removed. Zinn said this would result in a “chill on free speech caused by the secret surveillance of citizens.” See generally HOWARD ZINN, DECLARATIONS OF INDEPENDENCE: CROSS-EXAMINING AMERICAN IDEOLOGY 182-230 (1991).

108 Schauer, supra note 104, at 689.

109 Id. at 690.

110 Id. at 691. This would be in addition to the negative ban on government abridgement.

111 Id.

112 Id. at 692.
where citizens must evaluate whether an expression or action treads too close to prohibited speech—rather than altering specific behaviors, is the real indicator of the chilling effect.113

Raymond Shih Ray Ku, in his 2002 *Minnesota Law Review* article, argued that in order for free expression to survive, citizens understand a “reasonable expectation of privacy” in developing their personal beliefs.114 Ku said the Fourth Amendment does not just protect privacy: it is a “means of preserving the people's authority over government.”115 With electronic surveillance, this expectation is always shifting because rare technologies quickly become commonplace before the average citizen is familiar with their existence and implementation.116

In his 2007 *New York University Law Review* article, Daniel Solove argued that the First Amendment should protect against the government gathering information on citizens’ First Amendment activities.117 Solove said First Amendment protections should restrict government information gathering if there is a “discernible” chilling effect on constitutionally protected activities.118 Solove said, however, that it is difficult to establish an actual chilling effect because it is “hard to measure the deterrence caused by a chilling effect.” He said this is because “it is impossible to determine with certainty what people would have said or done in the absence

---

113 *Id.* at 731.


118 *Id.* at 154.
of the government activity.” 119 Solove said the only evidence of a chill would be the “person’s own assertions that she was chilled.” If the Court accepted this claim at face value, Solove said it would allow anyone to establish a chilling effect in any situation.120

Katherine Strandburg, in a 2007 Boston College Law Review article, argued that the First Amendment’s protections for freedom of association provide a “framework” for regulating “relational surveillance.”121 Strandburg used the term “relational surveillance” to refer to the computer analysis of “noncontent traffic data to map networks of associations.”122 Strandburg was concerned with threats to association, as opposed to the government “listening in” on communication content.123 Strandburg said that there is a “potential chilling effect” when the government uses relational surveillance to monitor citizens.124 She said the First Amendment’s guarantee for freedom of association must be seen as a unique consideration in evaluating relational surveillance programs —separate from the Fourth Amendment’s protections from unreasonable search and seizure.125 Strandburg said government mining of databases—containing information on communication patterns—might reveal citizens’ “exploratory activities” in Internet search patterns. She said this could “mark an individual” as a member of an association before they ever officially joined it.126 Strandburg concluded that the First

119 Id. at 155.
120 Id.
122 Id. at 741.
123 Id. at 749, n. 9.
124 Id. at 747.
125 Id. at 748.
126 Id. at 752.
Amendment’s right to freedom of association should limit relational surveillance by the government if it “amounts to disclosure of expressive associations.”\textsuperscript{127}

Matthew Lynch, in his 2007 \textit{First Amendment Law Review} article, creates a hypothetical “Orwellian Act” to evaluate the constitutionality of government restriction on a speaker’s right to choose his or her audience.\textsuperscript{128} Lynch’s “Orwell Act” is an imagined “extraordinary legislative response to public demand for greater security” in response to the 9/11 terrorist attacks. The Orwell Act would allow the government, in the name of national security, to monitor “every communication by verbal or technological means.”\textsuperscript{129} Lynch identified this action as an “Orwellian loophole” where the government could monitor speech between the speaker and his or her private audience.\textsuperscript{130} He called the loophole a “widening crack between Fourth Amendment, First Amendment, and right-to-privacy protections.”\textsuperscript{131}

Lynch identified one of the issues in “chilling-effect” claims by plaintiffs in court cases. He said that in order for plaintiffs to successfully argue their speech was concretely chilled, they must show that they were afraid to speak out against the government because of fear of punishment. However, this fear is invalidated as a claim if they are speaking out in court.\textsuperscript{132} Lynch said that in order to prove a “chill” plaintiffs would need to show the chill resulted from actual government surveillance, not just perceived potential surveillance.\textsuperscript{133} Lynch called for a

\textsuperscript{127} Id. at 819-20.


\textsuperscript{129} Id. at 239, 242.

\textsuperscript{130} Id. at 236.

\textsuperscript{131} Id. at 240.

\textsuperscript{132} Id. at 267.

\textsuperscript{133} Id. at 272.
new approach to where “government surveillance is an act directed at speech itself, rather than its secondary effects or its time, place, and manner.”\textsuperscript{134}

Lynch discussed the nature of anonymous speech and how it creates new theory of relationships between speaker, the contents of the speech, and the intended audience.\textsuperscript{135} Lynch used sociology studies from the 1950’s to argue that a speaker will change his or her message depending upon who they believe the recipient of the communication will be.\textsuperscript{136} Lynch applied the Hawthorne Effect—a psychological term referring to the result of 1920’s research on Chicago factory workers showing that when workers knew they were being watched, their work output improved—to surveillance to argue that government surveillance can change speakers communications.\textsuperscript{137} He said, “Years of expression subject to known observation may subconsciously condition speakers toward a pattern of behavior designed to please the full audience.”\textsuperscript{138} This would include the uninvited observer, as well as the intended audience.\textsuperscript{139}

Lynch concluded his article by calling on the Supreme Court to “recognize that a speaker’s choice of audience is as fundamental to speech as the speaker’s choice of words, choice of medium, and choice to speak at all.”\textsuperscript{140}

\textsuperscript{134} Id. at 289.
\textsuperscript{135} Id.
\textsuperscript{136} Id. at 289-90.
\textsuperscript{137} Id. (citing D. Michael Risinger et al., The Daubert/Kumho Implications of Observer Effects in Forensic Science: Hidden Problems of Expectation and Suggestion, 90 CAL. L. REV. 1 (2002)).
\textsuperscript{138} Id.
\textsuperscript{139} Id.
\textsuperscript{140} Id.
Breathing Space

William Banks, in his 2000 *American University Law Review* article on national security surveillance, said that the idea of “breathing space” as a First Amendment concept arises from the need for privacy in group association.141 When a group “espouses dissident beliefs,” it is more likely to be the target of government surveillance due to national security concerns.142 Banks recognized the development of the “breathing space” concept in case law:

The idea that associational privacy provides an individual "breathing space" has often been an issue in national security surveillance case law since the late 1950s, albeit not always the basis for overturning government surveillance.143

Banks said that any use of domestic surveillance has the potential to “chill” First Amendment expression.144 Banks said this intersection of domestic security and freedom of expression is balanced by two “analytic devices”: 1) the courts isolate certain categories of expression as having “little or no value” such as “incitements to violence” and “publication of information likely to cause irreparable harm to the national security” and 2) the courts ask whether “expressive interests” were targeted or only an “incidental by-product” of government operations.145 He referred to this latter analytic device as a “purpose or effect” analysis that creates a “subjective inquiry” when surveillance activities are challenged.146

142 *Id.*
143 *Id.* at 45.
144 *Id.* at 6.
145 *Id.*
146 *Id.*
Banks said that the First Amendment should not be “a barrier to government surveillance activity” unless the intention of surveillance is the “chilling” of “protected expression.”\textsuperscript{147} He said that surveillance might also be challenged when there is a “confluence of interests” protected by the First and Fourth Amendments:

Problems arise, however, at the intersection of First and Fourth Amendment interests, where protected expression may be chilled by surveillance of groups or individuals selected on the basis of advocacy of unpopular views, or where individuals are associated with a terrorist group on the basis of religious, ethnic, or national affiliation.\textsuperscript{148}

He gave the example of “intrusive surveillance…alleged to have chilled the exercise of protected expressive activities.”\textsuperscript{149} Hill said that whether or not surveillance occurs, the existence of “surreptitious recording… of individual communication” can create suspicion, which chills free expression.\textsuperscript{150}

J.L. Hill, in his 2004 \textit{Boston College Law Review} article on constitutional thought, identified three political values –privacy, autonomy and self-expression— which give life to the concept of breathing space as a political value in Democracy.\textsuperscript{151} Hill said

Privacy provides the self shelter from the storm; it gives the nascent self the breathing space to develop, and the developed self a personal realm to exist as it is, free from the prying eyes and corrosive influences of society.\textsuperscript{152}

The right to unrestricted expression in private discourse allows the private citizen to develop fully.\textsuperscript{153} Autonomy acts as a catalyst in the development of individual choice. When

\begin{thebibliography}{99}
\bibitem{147} \textit{Id.} at 6.
\bibitem{148} \textit{Id.} at 6. 122.
\bibitem{149} \textit{Id.} at 7.
\bibitem{150} \textit{Id.} at 38.
\bibitem{152} \textit{Id.} at 575.
\end{thebibliography}
citizens can privately engage in interpersonal communication on meaningful issues, they are free to explore ideas that fall outside the bounds of accepted doctrine. Alternative ideas are born from these private interactions—once developed, they can be introduced into the marketplace through public self-expression. Hill identified self expression” as the “soul” of freedom.\textsuperscript{154} Therefore, the political values of privacy, autonomy and self-expression enable democratic citizens to manifest their personal beliefs as political values.\textsuperscript{155}

**Surveillance Societies (Dystopian and Utopian Visions)**

As discussed in the previous two sections, scholars have suggested that government surveillance programs may have a chilling effect on free speech in the marketplace when it restricts citizen’s perceived breathing space for expressing socially unpopular political ideas. Surveillance may also have the potential to undermine citizen’s assessment of the privacy of their communications when they may not be certain of the extent of programs and technologies employed by the government. Fictional surveillance societies can be used as a model to explore the First Amendment theories on the “chilling effect” and the marketplace of ideas. Many authors have explored scenarios of governance where citizens do not enjoy protections for democratic values such as free speech and privacy. These examples from literature share the common theme of an oppressive regime, which restrains citizens’ speech through surveillance practices that undermine political expression by intimidating citizens who have unpopular or subversive viewpoints.

Surveillance societies are often based on the idea that widespread monitoring will limit subversive activities and promote lawfulness among citizens. Although this idealized goal in

\textsuperscript{153} Id.

\textsuperscript{154} Id.

\textsuperscript{155} Id.
monitoring individual’s communications is often motivated by government’s justification that it improves society, monitoring may also have a negative effect, destroying the political principles that foster freedom and Democracy. This approach, often meant to quiet revolutionary movements and promote domestic security, has been most thoroughly explored by philosophers and novelists. John Stuart Mill is notable for introducing the word “dystopia” to characterize a society that falls from the classical Democratic ideals for governance. Although Mill lived in a time when mass surveillance was technologically impossible, his ideas are directly applicable to the erosion of liberty and free expression in a surveillance society.

In an 1868 speech on Ireland before Parliament, Mill used the phrase “dystopian” to characterize the antithesis of Utopia as envisioned by St. Thomas More. More’s Utopia represented an idealized fictional society with a perfect legal and social system. Mill’s play on the Latin word “utopia” was a commentary on the social ills of the day. Coupled with his advocacy of the open exchange of ideas, it is likely that Mill would see government suppression of the marketplace of ideas as a dystopia. Fictional surveillance societies can be characterized as dystopian in nature, straying from their idealistic visions in their real-world application. This struggle over whether surveillance creates a utopian or a dystopian society is the key difference between Bentham’s Panopticon and Nineteen-Eighty-Four by George Orwell.


157 MORE, supra note 156.

Jeremy Bentham published *Panopticon* in 1787. The panopticon was a prison that would allow all prisoners (pan) to be watched (opticon) without ever giving the appearance that they were being observed. In this way, the prisoners could never tell when they were being watched. In Bentham’s Panopticon, it would seem that the prisoners were always being watched and therefore they would be less likely to engage in deviant acts because they would be deceived by a “sentiment of an invisible omniscience.” Although Bentham volunteered to pay for the prison and serve as an unpaid warden, his design was never adopted by Parliament.

George Orwell’s 1949 book *Nineteen-Eighty-Four* is a fictional account of Winston Smith, a man who lives in a totalitarian society called Oceania. In the novel, a totalitarian regime—Big Brother—operates as a surveillance society using a security elite known as the “thought police” to detect and punish critical views, or “thought crimes.” Smith is a middle class bureaucrat who struggles with his existence in a surveillance society under a dictator known as Big Brother. In the book, Oceania is always at war and the “inner party” maintains tight social controls to limit dissent. Smith keeps an illegal secret diary of his thoughts that are critical of Big Brother.

Even though all citizens are monitored in their homes by telescreens, Smith strategically positions himself in a corner of the room where he is beyond the sight of the screen when writing in his diary. These cameras—connected to telescreens—along with hidden microphones, are monitored by the thought police, a secretive law enforcement organization that tortures and kills any person found to threaten the Big Brother through departure from official government.

---


160 *Id.*

positions. Smith and his heroine, Julia, operate under the false assumption that they have privacy. In the end, they realize that this is just an illusion and they are detained and tortured by the thought police.

Bentham envisioned a surveillance society, at least in a penal system, as a beneficial arrangement that would promote better behavior. Orwell portrayed omnipresent surveillance as oppressive to citizen behavior. In both stories, the characters obey the government because they are aware that they are being watched at all times.162

Contemporary scholars use the Orwell vision in Nineteen-Eighty-Four to produce commentary on modern surveillance practices. David Lyon, in his 1994 book, The Electronic Eye, traced social and academic reflection on the Nineteen-Eight-Four scenario since the early 1970s in his book on surveillance societies.163 Lyon is a professor of sociology at Queens University. He is also the Director of The Surveillance Project, a policy research group that studies surveillance from an interdisciplinary approach.164 Lyon concludes that a “total surveillance society” as envisioned by Orwell would be limited only by technological capabilities.165

---

162 Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. CAL. L. REV. 1083, 1101-02 (2002). See also Nancy Chang, Center for Constitutional Rights, The USA PATRIOT ACT: What's So Patriotic About Trampling on the Bill of Rights? (2001) (on file with the author). Beyond metaphorical comparisons, authors have consistently linked First Amendment protections of free expression to Fourth Amendment privacy protections. In the post-PATRIOT era, changes in surveillance laws can be seen in the light of an assault on privacy rights. Nancy Chang suggests that there has been a three-prong assault that challenges not only privacy, but First Amendment protections for political association and the freedom to dissent: 1) The government has unprecedented surveillance power; 2) In the name of national security, law enforcement is allowed to monitor the Internet and use wiretaps; 3) Information is freely exchanged between criminal and intelligence agencies.


165 Lyon, supra note 163 at 57.
Lyon said that the *Nineteen-Eight-Four* scenario has been “superceded technologically” by globalization of surveillance activities. He argued that Bentham’s *Panopticon* is the dystopian prophecy that most accurately reflects how modern surveillance societies truly operate. Lyon said Bentham believed that the Panopticon would have a positive effect on the prisoners who were being monitored. This is a far cry from the Big Brother surveillance imagined in *Nineteen-Eighty-Four*.

Lyon suggested that it is important to pay attention to both the Orwellian and Panoptic models in order to understand surveillance and find possible “alternative models” for controlling subversive behaviors. The Panopticon is a very elegant, yet antiquated approach to surveillance. Orwell’s vision incorporates “information technology” to collect and store data on individuals. Both models are based on the unperceivable surveillance that creates uncertainty among the observed. In both Bentham and Orwell’s scenarios, the observed must know that someone is watching them in order for citizen’s to alter their behavior as part of the chilling effect. In Bentham’s Panopticon and Orwell’s Big Brother society both rely on citizens being aware of surveillance, but being unable to judge the extent of the secretive surveillance beyond the technological devices they can see—such as the cameras in watching Winston Smith in Orwell’s story. As Lyon said bluntly, “You simply comply, because you never know when “they” might be watching.” Lyon also linked Orwell’s handling of surveillance societies to a degradation of human dignity. It is not just privacy that is at issue; it is the loss of the essential human right to

166 Id.
167 Id.
168 Id.
169 Id.
170 Id.
self-respect through the exercise of critical thinking in evaluating conflicting information and points of view.171

The literature on surveillance is rife with metaphorical comparisons to Orwell’s extreme scenario. Authors have linked contemporary surveillance practices to the creation of a “Big Brother” totalitarian regime. Most of these links, at least recently, focus on Internet and commercial data collection as tools for governments and corporations seeking to more closely monitor citizen’s economic and social activities. James Nehf’s 2003 Washington Law Review article on information privacy compared modern data collection systems to the tactics of the fictional authoritarian regime in Nineteen-Eighty-Four. People often fear a negative consequence from data collection, even when the information collected is “mundane and harmless.”172 Modern data collection systems “limit freedom by tightening the government’s hold over various aspects of citizens’ private lives.” Nehf used the metaphor of Jeffrey Bentham’s Panopticon, suggesting that mass surveillance “curtails free will.”173

Stan Karas, in his 2005 Albany Law Journal of Science and Technology article, evoked images of “telescreens” as depicted in Nineteen-Eighty-Four.174 He said this sort of “all-seeing eye of the state” creates a privacy problem by encouraging citizens to abandon their privacy in exchange for the “favor of disclosure.” Karas narrowly examined the surveillance and disclosure of personal data as it relates to identity theft. He said that data collection—the electronic monitoring of consumer’s financial records—by private corporations has a negative impact on

171 Id.


173 See also Margaret Raymond, Rejecting Totalitarianism: Translating the Guarantees of Constitutional Criminal Procedure, 76 N.C. L. REV. 1193 (1998). Margaret Raymond said that totalitarian regimes collect private information to create fear in the populous resulting in a chilling effect on free expression.

the democratic process. Karas’ article focused on surveillance by businesses, which has only recently begun to be seen by scholars as a threat to the democratic process. However, Karas’ reasoned that when citizens complacently go along with this monitoring, there is a climate created where there is a “favor of disclosure” and citizens no longer expect strong privacy protections from monitoring of their personal data.

Surveillance can be interpreted by a society as a valuable tool for protecting security or a harmful strategy for suppressing human rights and political involvement. Often, a society’s view of surveillance—and consequently its interpretation of the legality of such a program—depends entirely upon contemporary circumstances. In the United States of the 21st century, the September 11th attacks and the War on Terror were circumstances that demanded the country’s attention.

American Public Sentiment

One factor influencing the balance of protections for electronic surveillance is public sentiment. If the public is willing to accept executive programs, then may be less pressure for representatives in Congress to investigate or update surveillance laws. When there are public concerns over government programs, there may be pressure for intelligence investigations or updated legislation. Little polling data is available for public opinion on electronic surveillance. The first polling data from the communist era of the 1950’s and 1960’s will be presented, followed by a collection of polling data collected after the 2005 revelation of warrantless wiretapping by the American government.

Thomas Emerson, in his 1963 *Yale Law Review Journal* article, discussed a 1953 Gallup poll of public support for freedom of expression. In relating the poll data to his theory of key values in protecting the First Amendment, Emerson said the results revealed “an alarmingly high proportion of the population who are unwilling to apply the basic principles of the theory in practice.” In the Gallup poll, sixty-seven percent of respondent thought that a person “known to favor communism” should not be allowed to make a speech in their city of town. Emerson said that just twenty-nine percent thought that a person “known to favor communism” should be permitted to speak.

Emerson also cited a 1955 study by Samuel Stouffer that found “the willingness to grant freedom of speech to Communists was a function, less of political views or economic status, than on the degree of education.”

More polling data is available for assessing the 21st century sentiment of Americans in regards to current government surveillance programs. Many polls relating to the Terrorist Surveillance Program were commissioned after the 2005 revelation of the domestic wiretapping program. It is important, in each of the polls, to remember the political agenda of the organization that commissioned the poll, as well as limited samples.

A poll conducted by Zogby International in January of 2006 interviewed 1,216 United States adults. In response to the statement, "If President Bush wiretapped American citizens without the approval of a judge, do you agree or disagree that Congress should consider holding

---


177 *Id.*


him accountable through impeachment,” fifty-two percent of respondents agreed, while forty-three percent disagreed and six percent didn’t know or declined to answer. Just over half of respondents favored impeaching the President for his actions.

A January 2006 poll conducted jointly by the Associated Press and Ipsos found that fifty-six percent of respondents agreed that the government should get a court warrant before eavesdropping on calls and e-mails of U.S. citizens overseas who are believed to be linked to terrorism. Of those polled, forty-two percent did not believe court approval is not necessary. This data reflects the split in public sentiment toward the program found in the Zogby poll on impeachment. A large percentage of respondents are in favor of warrantless domestic surveillance programs.

NBC and the Wall Street Journal commissioned a poll through Hart/McInturff, which was released in late January of 2006. When asked if they approved or disapproved with the Bush Administration’s approach to wiretapping without court order, fifty-one percent of respondents approved of the approach, forty-six percent disapproved and three percent were not sure. This supports the AP-Ipsos polling data on warrantless surveillance. In regards to the wiretapping of American citizens with suspected terrorist ties, forty-one percent of respondents said they believed the administration should be able to conduct wiretaps without a court order, while fifty-three percent said that a court order should be required (four percent said it “depends,” two percent were unsure.) When asked how concerned they were that the Bush administration’s unwarranted wiretaps could be “misused to violate people’s privacy,” thirty-one percent of


53
respondents were “extremely concerned,” twenty-five percent “quite concerned,” twenty-two percent “not really concerned,” twenty-one percent “not concerned at all,” and one percent were unsure. American sentiment in regards to valuing privacy, at least as indicated by this poll, seems to reflect only mild concern for violation of statutes requiring warrants for surveillance.

A CNN/USA Today/Gallup poll of 1000 American adults was released in February of 2006 revealing that about a fifth of Americans think federal agents have listened in on their phone calls. It is interesting that given the media coverage, and executive branch acknowledgements of widespread surveillance dragnets, that only a fraction of citizens acknowledge they may have been targets. The poll also showed that respondents were split as to whether President Bush’s Terrorist Surveillance Program was legal—forty-nine percent felt the president had “definitely or probably broken the law by authorizing the wiretaps,” while forty-seven percent said he “probably or definitely had not.” This split was mirrored in the question asking whether the program was right or wrong, with forty-seven percent saying it was right and fifty percent saying it was wrong.

A Harris Interactive poll commissioned by the American Bar Association in February of 2006, asked participants “In the fight against terrorism, which of the following reasons, if any, would justify the government eavesdropping on your personal communications, including phone calls or emails, without a search warrant or court order?” Of the respondents, forty-eight percent felt the government was justification in monitoring communications. Breaking down the forty-eight percent, respondents felt the following reasons were justification: twenty-two percent

---

182 Poll: Fifth of Americans think calls have been monitored, CNN.com, Feb. 14, 2006, http://www.cnn.com/2006/POLITICS/02/14/poll.wiretaps/index.html (last visited June 22, 2008). The sampling error for those questions was plus or minus 5 percentage points. 1,045 adults were polled by phone.

183 Harris Interactive, American Bar Association’s Presidential Power Datasheeted Questionnaire (Feb. 7, 2006), available at http://www.abanet.org/media/docs/surveillancepoll06.pdf. 1,045 completed interviews with adults 18+, plus or minus 3 percents.
said an anonymous tip of helping to plan a terrorist attack was justification, twenty-one percent said suspicion of sending money to a terrorist organization was justification, eight percent felt membership or support of an organization publicly criticizing the president was justification, while thirteen percent said that the “government does not need to give any special reason to monitor your personal communications.” Of the respondents, forty-five percent said that the government was never justified in eavesdropping on personal communications without approval by a court of Congress (five percent responded they didn’t know or were not sure, while two percent declined to answer). Again, the data from this poll mimics the results from the other polling organizations.

A February 2006 Pew Research Center Poll found that fifty-four percent of American believe it is “generally right for the government to monitor communications of Americans suspected of having terrorist ties without first obtaining permission from the courts.” Of the respondents, fifty percent felt that the government hadn’t yet gone far enough in protecting the country against terrorism, while just thirty percent felt concerned about government restriction of civil liberties.

An outlier in the collection of polls can be found in data collected from a study commissioned by the ACLU, one of the organizations that filed a case against the government program. In January of 2008, the American Civil Liberties Union commissioned the Mellman Group to conduct a poll on domestic surveillance. Of those polled, sixty-three percent favored

---


185 The Mellman Group, Voters Vigorously Oppose Warrantless Wiretaps, Blanket Warrants, And Immunity For Telecom Communities (Jan. 18, 2008), available at http://www.aclu.org/pdfs/safefree/mellmansurvey_jan2008.pdf. 1,000 “likely voters” in the 2008 general election were interviewed, with a 3.1 percent margin of error.
“requiring the government to obtain a warrant from a court before wiretapping the conversations U.S. citizens have with people in other countries. Of those polled, fifty-five percent strongly support warrant requirements, while just thirty-three percent support warrantless wiretapping of Americans’ international conversations. When asked whether they opposed allowing courts to issue blanket warrants for wiretapping American citizens without naming a specific individual, fifty-eight percent of respondents strongly opposed blanket warrants, while thirty-three percent supported them. Of the respondents, fifty-seven percent “reject immunity for phone companies that may have violated the law by selling customers’ private information to the government, preferring to let courts decide the outcome of any case.” This data is unique in that it was collected in 2008, after Congressional investigations into domestic surveillance, yet it must be considered carefully given the potential bias of the sponsoring organization.

Cumulatively, the data collected from these polls indicates that the American public is not very concerned about the government’s use of electronic surveillance on American citizens. Most citizens seem to trust the government’s intentions in carrying out surveillance. Whether this is based on a faith in compliance with statutory requirements, or rather, a sense of Patriotism in protecting national security is unclear. The attitude does seem significant given the strong suspicion of government search and seizure that was prevalent during the American Revolution and the drafting of the Constitution.

**Research Questions**

Research was conducted to evaluate the connection between electronic surveillance and free speech in an age of terrorism. The proposed questions for this research are:

1. What is the legislative history governing the surveillance of United States citizens?
2. What is the judicial history of the relationship between political surveillance of citizen communications and those citizens’ First Amendment rights?
3. How does the Fourth Amendment’s protection for privacy relate to the First Amendment’s protections for free speech?

4. Do current surveillance cases in the courts show a trend of protection for Emerson’s key First Amendment values, or a shift towards Lasswell’s garrison state?

5. What is the current balance between the need to protect civil liberties and the need to protect national security based on judicial interpretations of federal surveillance laws?

6. Does government surveillance of private communications create a chilling effect on free expression in the marketplace of ideas, as interpreted by the courts?

**Methodology**

This dissertation uses the methodology of legal research. Primary resources, including primarily federal statutes, cases, executive orders, as well as agency policies, rules and regulations regarding the First Amendment and surveillance were examined.

Search Strings for online sources such as Lexis/Nexis, the FCC’s website, and Google included:

- “electronic surveillance”
- “domestic spying”
- “electronic surveillance” and “free speech”
- “electronic surveillance w/10 chilling effect”
- “domestic spying” and “chilling effect”
- “electronic surveillance w/10 First Amendment”
- “domestic electronic surveillance”
- “chilling effect w/10 free speech”
- “surveillance societ*”
- “marketplace of ideas” and “surveillance”
- “First Amendment” and “marketplace of ideas”
- “breathing space”
- “Foreign Intelligence Surveillance Act”
- “Terrorist Surveillance Program”

Federal statutes were reviewed looking for laws that govern electronic surveillance of the telecommunications networks, as well as laws that suppress or punish political speech. From this initial list of statutory law, cases were identified that involved the issues of electronic surveillance, free speech or the marketplace of ideas. Executive orders pertinent to past and
current surveillance initiatives were also identified. Statutes, cases and executive orders were accessed using the Lexis-Nexis Database.

Case names and names of secondary source authors were added as research progressed. Law reviews published before 1960 were reviewed using printed copies, as they are not available on the Lexis/Nexis database.

Additionally, secondary sources such as seminal works on the First Amendment, bibliographies from recognized experts such as Leonard Levy, as well as historical texts and accounts of the National Security Agency were examined. The history of the telecommunications network providers was examined. Theses sources were identified using key word searches in the University of Florida library database.

In this way, the dissertation research process allowed the researcher to summarize the legal framework, explore current issues related to this framework and review theoretical connections between the ideas of free speech and national security. The legal sources were also used to explore a new theoretical construct explaining how the nation’s shift towards protecting security, paired with society’s expanding technological capabilities, has created a new sort of citizen-government relationship that could modify the application of constitutional protections. These changes will be analyzed using constitutions, statutes and case law.

**Definitions**

The definitions in this section come from Black’s Law Dictionary. They are provided to give the reader a starting point in understanding the laws governing electronic surveillance, which will be discussed in the next chapter. The definitions will also be a starting point for interpreting the language of the court decisions presented in chapter three.
Bugging: A form of electronic surveillance by which conversations may be electronically intercepted, overheard, and recorded, usu[ally] covertly; eavesdropping by electronic means.\textsuperscript{186}

Chilling Effect: 1. Constitutional law. The result of a law or practice that seriously discourages the exercise of a constitutional right, such as the right to appeal or the right of free speech. 2. Broadly, the result when any practice is discouraged.\textsuperscript{187}

Civil Liberty: Freedom from undue governmental interference or restraint. This term usu[sually] [r]efers to freedom of speech or religion.\textsuperscript{188}

Conspiracy: An agreement by two or more persons to commit and unlawful act; a combination for an unlawful purpose. In criminal law, conspiracy is a separate offense from the crime that is the object of the conspiracy.\textsuperscript{189}

Domestic: 1. Of or relating to one’s own country <domestic affairs>. 2. Of or relating to one’s own jurisdiction.\textsuperscript{190}

Eavesdropping: The act of secretly listening to the private conversations of others without their consent.\textsuperscript{191}

Electronic surveillance: references definition of eavesdropping.\textsuperscript{192}

Espionage: The practice of using spies to collect information about what another government or company is doing or plans to do.\textsuperscript{193}

General warrant: 1. A warrant issued by the English Secretary of State for the arrest of the author, printer, or publisher of a seditious libel, without naming the persons to be arrested. 2. A warrant that gives a law-enforcement officer broad authority to search and seize unspecified places or persons; a search or arrest warrant that lacks a sufficiently

\textsuperscript{186} BLACK’S LAW DICTIONARY 189 (7th ed. 1999).

\textsuperscript{187} Id. at 233.
\textsuperscript{188} Id. at 239.
\textsuperscript{189} Id. at 305.
\textsuperscript{190} Id. at 529.
\textsuperscript{191} Id. at 529.
\textsuperscript{192} Id. at 537.
\textsuperscript{193} Id. at 565.
particularized description of the person or thing to be seized or the place to be searched.\textsuperscript{194}

Liberty: 1. Freedom from arbitrary or undue external restraint, esp. by a government. \textit{<Give me liberty, or give me death>}. 2. A right, privilege, or immunity enjoyed by prescription or by grant; the absence of a legal duty imposed on a person \textit{<the liberties protected by the Constitution>}.\textsuperscript{195}

Marketplace of ideas: A forum in which expressions of opinion can freely compete for acceptance without governmental restraint. Although Justice Oliver Wendell Holmes was the first jurist to discuss the concept as a metaphor for explaining freedom of speech, the phrase \textit{marketplace of ideas} dates in American case law only from 1954.

Natural liberty: The power to act as one wishes, without any restraint or control, unless by nature.\textsuperscript{196}

Negative Right: A right entitling a person to have another refrain from doing an act that might harm the person entitled.\textsuperscript{197}

Pen register: A mechanical device that logs dialed telephone numbers, without overhearing the telephone conversation, by monitoring electrical impulses.\textsuperscript{198}

Penumbra: A surrounding area of periphery of uncertain extent. In constitutional law, the Supreme Court has ruled that the specific guarantees in the Bill of Rights have penumbras containing implied rights, esp. the right of privacy.\textsuperscript{199}

Personal liberty: A person’s freedom to do as one pleases, limited only by the government’s right to regulate the public health, safety, and welfare. ---Also termed individual liberty.\textsuperscript{200}

Political liberty: A person’s freedom to participate in the operation of government, esp. in the making and administration of laws.\textsuperscript{201}

\textsuperscript{194} Id. at 1579.
\textsuperscript{195} Id. at 931.
\textsuperscript{196} Id. at 930.
\textsuperscript{197} Id. at 1323.
\textsuperscript{198} Id. at 1155.
\textsuperscript{199} Id. at 125.
\textsuperscript{200} Id. at 1164.
Positive Right: A right entitling a person to have another do some act for the benefit of the person entitled.\textsuperscript{202}

Prior Restraint: A governmental restriction on speech or publication before its actual expression. Prior restraints violate the First Amendment unless the speech is obscene, is defamatory, or creates a clear and present danger to society.\textsuperscript{203}

Spy: One who secretly observes and collects secret information or intelligence about what another government company is doing or plans to do; one who commits espionage.\textsuperscript{204}

State Secrets privilege: A privilege that the government may invoke against the discovery of a material that, if divulged, could compromise national security. Also termed national-security privilege.\textsuperscript{205}

Surveillance: Close observation or listening of a person or place in the hope of gathering evidence.\textsuperscript{206}

Warrant: A writ directing or authorizing someone to do an act, esp[ecially] one directing a law enforcer to make an arrest, a search or a seizure.\textsuperscript{207}

Wiretapping: The electronic or mechanical eavesdropping, usu[ally] done by law-enforcement officers under court order, to listen to private conversations.\textsuperscript{208} Wiretapping is regulated by federal and state law, and is often shorted to “tapping.

\textbf{Summary of Chapters}

Chapter two provides a comprehensive overview of the legislative history of electronic surveillance in the United States beginning with the Radio Act of 1912 through the current
legislative actions to update the Foreign Intelligence Surveillance Act. Chapter two also
provides a history of electronic surveillance as it has operated outside of the legal framework,
beginning with military surveillance programs in the early part of the 20th century. The chapter
looks at each law chronologically, with special emphasis on how the statute modified definitions
of terms, warrant requirements and other provisions governing surveillance.

Chapter three provides a case-by-case look at the major judicial decisions involving First
Amendment principles such as the “chilling effect” and “breathing space,” as well as Fourth
Amendment cases interpreting the application of surveillance law. Chapter three also highlights
cases decided on Fourth Amendment grounds, which have implications for First Amendment
protections.

Chapter four discusses the Bush Administration’s Terrorist Surveillance Program and court
cases filed since the disclosure of the Terrorist Surveillance Program. The chapter looks at three
cases, selected for their relevance to the discussion of the relationship between First and Fourth
Amendment protections for surveillance.

Chapter five is the conclusion. In chapter five, each of the research questions are answered
based on the data collected. Findings are offered answering the research questions. Chapter five
concludes with considerations and recommendations for remedies and future research.
CHAPTER 2
LEGAL HISTORY OF DOMESTIC SURVEILLANCE BY US GOVERNMENT

The legal background of electronic surveillance by the government spans almost a century, dating back to World War I. The first United States intelligence operation, the Black Chamber, was initiated before The Radio Act of 1912 codified telecommunications regulation. Since that time, a complex body of statutes has been written and revised to address changing technologies and concerns over government acquisition of telecommunications content. This chapter will look at the history of the Black Chamber during World War I, The Communications Act of 1934, the creation of the National Security Agency, the Omnibus Crime Control and Safe Streets Act of 1968, the Foreign Intelligence Surveillance Act of 1978, the Electronic Privacy Communications Act of 1986, the Communications Assistance for Law Enforcement Act of 1994, The Telecommunications Act of 1996, The USA PATRIOT Act of 2001 and subsequent updates to the PATRIOT Act. Each of these laws will be looked at in a chronological analysis, introducing the act and its effects as it modifies existing electronic surveillance law at the time of its passage.

The Black Chamber

U.S. intelligence traces its roots back to 1917 when the country entered World War I (WWI). At that time, the U.S. War Department began intercepting coded messages across international lines. This operation became known as the “American Black Chamber” and it was maintained by first the State Department, and then the War Department, beyond the end of the WWI.

---

1 HERBERT O. YARDLEY, THE AMERICAN BLACK CHAMBER (1931).
2 Military Intelligence Section 8 (MI-8).
3 YARDLEY, supra note 1.
In 1919, the Black Chamber set up offices in New York City under the name of The Code Compilation Company. The program lasted for ten years before Secretary of State Henry B. Stimson ended it in 1929. At that time, Osborne Yardley, a key player in the Black Chamber, rebelled against Stimson by writing a tell-all book. The book reveals that government agents visited the major telegraph companies and requested copies of all foreign government cables. The legality of the Black Chamber surveillance operation would not be decided until the Church Committee investigated U.S. surveillance activities in the late 1970’s. This will be discussed later in this chapter.

The Radio Act of 1912

The Radio Act of 1912 was the first Congressional action to regulate federal wireless communication. It was passed in response to the sinking of the Titanic, as well as to address problems caused by amateur radio operators interfering with commercial and military messages. The Act went into effect four months from its passage on August 13, 1912. The Radio Act of 1912 outlawed “eavesdropping” on radio or cable traffic although this prohibition was suspended during the war. The major telegraphic companies were the Western Union Telegraph Company and the Postal Telegraph Company. Yardley’s account suggests that agents requested copies of all domestic cables. YARDLEY, supra note 1. See SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, 94TH CONG., SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, FINAL REPORT AT 1 (hereafter “CHURCH COMMITTEE FINAL REPORT”) (1976), available at http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIe.htm. The report discusses intelligence activities and operations during the 20th century. The report states that the FBI used 519 wiretaps and 186 microphone surveillances during 1945. It also states that until 1972, “the Bureau used wiretaps and bugs against both American citizens and foreigners within the United States—without judicial warrant—to collect foreign intelligence, intelligence and counterintelligence information, to monitor "subversive" and violent activity, and to determine the sources of leaks of classified information.” The report states that the CIA targeted 57 individuals with telephone wiretaps and microphones between 1947 and 1969. The report does not disclose numbers for the NSA, but states that it has been intercepting electronic communications since the 1950’s. The report states that the 1928 Olmstead decision (217 U.S. 438), discussed in chapter three, resulted in the FBI engaging in the “unrestricted use of wiretapping in both criminal and intelligence investigations.” Although the Radio Acts prohibited “eavesdropping,” on private communications, it wasn’t until the passage of the Communications Act of 1934, that the Supreme Court had an opportunity to extend this prohibition on eavesdropping to federal agents. Nardone v. United States, 302 U. S. 397 (1937); 308 U. S. 338 (1939). When Congress did restrict wiretapping, the report states that the Justice Department successfully argued that only the divulgence of contents of communications was prohibited, not the use of intercepted materials as evidence.

mandated licensing requirements for amateur radio operators and assigned channels for commercial, military and civilian transmissions. Licenses were required to specify 1) ownership and location of the station, 2) identification of station, 3) estimated wave length and range of transmissions, and 4) hours of station transmission. Responsibilities for licensing requirements and punitive fines were assigned to the United States Department of Commerce and Labor.  

The Radio Act of 1912 allowed the government to commandeer station equipment or control in times of national crisis:

Every such license shall provide that the President of the United States in time of war or public peril or disaster may cause the closing of any station for radio communication and the removal therefrom of all radio apparatus, or may authorize the use or control of any such station or apparatus by any department of the Government, upon just compensation to the owners.  

The nineteenth regulation of the Radio Act prohibited the disclosure of the contents of communications:

No person or persons engaged in or having knowledge of the operation of any station or stations, shall divulge or publish the contents of any messages transmitted or received by such station, except to the person or persons to whom the same may be directed, or their authorized agent, or to another station employed to forward such message to its destination, unless legally required so to do by the court of competent jurisdiction or other competent authority.  

Violation of this regulation was punishable by monetary fines or a prison sentence. The Radio Act defined “radio communication” as “any system of electrical communication by telegraphy or telephony without the aid of any wire connecting the points from and at which radiograms, signals, or other communications are sent or received.”

6 Id.
7 Id.
8 Id.
9 Id.
The Radio Act of 1927

The Radio Act of 1927 updated the statutes to include broadcasting, and assigned private radio communication to the AM band.10 The Radio Act of 1927, approved February 23, 1927, repealed the Radio Act of 1912.11 “Radio communication” was defined as “any intelligence, message, signal, power, pictures, or communication of any nature transferred by electrical energy from one point to another without the aid of any wire connecting the points from and at which the electrical energy is sent or received and any system by means of which such transfer of energy is effected.”12

The Radio Act of 1927, much like the Radio Act of 1912, allowed the President to commandeer stations during times of war, public peril, disaster, or national emergency. Like the 1912 Radio Act, this act prohibited divulging the contents of transmissions or receptions to “any person other than the addressee,” or his agent.13 The Act prohibited censorship of radio communications by prohibiting regulations that interfered with “free speech by means of radio communications” except in the case of “obscene, indecent, or profane language.”14

The 1927 Radio Act also created the Federal Radio Commission to replace the Commerce and Labor Department in regulating the United States’ radio spectrum in the public convenience, interest or necessity.15 The Federal Radio Commission was composed of five commissioners, appointed by the President, with Senate confirmation. The commission members elected the

---


12 Id. at § 32.

13 Id. at § 27.

14 Id. at § 29.

15 Id.
The FRC chairman. The FRC was charged with the responsibilities of: 1) classifying radio stations, 2) prescribing the nature of service for each station class, 3) assigning bands of frequencies or wavelengths for each station class, 4) determining station locations, 5) regulating station apparatus, 6) preventing interference between stations, 7) establishing zones of station service, 8) regulating chain broadcasting, 9) regulation station record keeping, and 10) holding hearings to enforce regulations of the Act. 16

The Communications Act 1934

The Communications Act of 1934 was the first comprehensive legislation to address the rapidly developing United States communications industry since the passage of the Radio Acts. 17 Enacted on June 19, 1934, the Act’s purpose was enabling a “rapid, efficient, nationwide, and worldwide wire and wire radio communication service” for all people. 18 The Act had six sections: 1) Title I established the Federal Communications Commission, outlining the agency’s divisions and powers; 2) Title II established common carrier regulations; 3) Title III outlined broadcast station requirements; 4) Title IV addressed judicial review of the communications industry; 5) Title V established guidelines for enforcement of the Act; and 6) Title VI addressed miscellaneous concerns such as amendments, cable television regulation and emergency war powers of the president. 19

16 Id. at § 4.


18 Commc’ns Act, 47 U.S.C. § 151 (1934). “For the purpose of regulating interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States a rapid, efficient, Nation-wide, and world-wide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of national defense, for the purpose of promoting safety of life and property through the use of wire and radio communications.” Id.

19 Id. Common carriers are defined as “telephone and microwave communications.”
In the Communications Act, common carriers are defined as entities that offer telephone and microwave communications service. The Communications Act defines several key terms relevant to understanding the framework of electronic surveillance that will be discussed in subsequent sections of this chapter:

1. **Wire communication**: “transmission of writing, signs, signals, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception of such transmission, including all instrumentalities, facilities, apparatus, and services (among other things, the receipt, forwarding, and delivery of communications) incidental to such transmission.”

2. **Interstate communication (transmission)**: “communication or transmission (1) from any State, Territory, or possession of the United States (other than the Canal Zone), or the District of Columbia, to any other State, Territory, or possession of the United States (other than the Canal Zone), or the District of Columbia, (2) from or to the United States to or from the Canal Zone, insofar as such communication or transmission takes place within the United States, or (3) between points within the United States but through a foreign country; but shall not... include wire or radio communication between points in the same State, Territory, or possession of the United States, or the District of Columbia, through any place outside thereof, if such communication is regulated by a State commission.”

3. **Foreign communication (transmission)**: “communication or transmission from or to any place in the United States to or from a foreign country, or between a station in the United States and a mobile station located outside the United States.”

4. **Common carrier**: “any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy, except where reference is made to common carriers not subject to this chapter; but a person engaged in radio broadcasting shall not, insofar as such person is so engaged, be deemed a common carrier.”

5. **Telephone exchange service**: “service within a telephone exchange, or within a connected system of telephone exchanges within the same exchange area operated to furnish to subscribers intercommunicating service of the character ordinarily furnished by a single exchange, and which is covered by the exchange service charge.”

---

20 *Id.* at § 153(a).

21 *Id.* at § 153(e).

22 *Id.* at § 153(f).

23 *Id.* at § 153(h).

24 *Id.* at § 153(r).
6. Telephone toll service: “telephone service between stations in different exchange areas for which there is made a separate charge not included in contracts with subscribers for exchange service.”25

The Communications Act of 1934 was the first law to define lawful and unlawful actions for common carriers. The Communications Act addresses discrimination and preferences by a common carrier, making it “unlawful” for a carrier to unjustly or unreasonably discriminate in regards to

charges, practices, classifications, regulations, facilities, or services for or in connection with like communication service, directly or indirectly, by any means or device, or to make or give any undue or unreasonable preference or advantage to any particular person, class of persons, or locality, or to subject any particular person, class of persons, or locality to any undue or unreasonable prejudice or disadvantage.26

Although large parts of the Communication Act are not relevant to a discussion of modern electronic surveillance, the act does address government and carrier cooperation in regards to communications service in its mandate for “franks and passes,” essentially free service provided by common carriers to governmental agencies in connection with national defense.27 The act authorizes common carriers to issue, give or exchange “franks and passes” with other carriers for the use of “their officers, agents, employees, and their families.”28 The act also authorizes common carriers to render free service to any government agency in “connection with the preparation for the national defense.”29

---

25 Id. at § 153(s).
26 Id. at § 202(a).
27 Id. at § 210(a).
28 Id. at § 210(b).
National Security Agency

In 1945, the U.S. entered World War II and all telegraph messages were intercepted under a government program known as Operation Shamrock. This program, which grew out of the Black Chamber operation discussed earlier in this chapter, was not legally authorized by any statute or executive action, but rather was a military intelligence operation.

It wasn’t until 1952 that communications surveillance was assigned to a specific agency. At that time, President Harry Truman sent a seven-page top-secret memo to Secretary of State Dean G. Acheson and Secretary of Defense Robert A. Lovett establishing the National Security Agency. The memo outlined the functions of the NSA to include: 1) protecting “Communications Security” (COMSEC) of United States telecommunications that are national security related and 2) obtaining foreign intelligence related telecommunications through the interception of “Signals Intelligence” (SIGINT). SIGINT is the gathering of electronic intelligence signals such as radio transmissions. It is a combination of communications intelligence (COMINT) and electronic intelligence (ELINT). COMINT is the specific type of SIGINT that involves interception of human-encoded messages between people using devices such as telegraphs, phones, radios or computers. ELINT involves interception of transmission from electronic devices, such as radar. The original purpose of the NSA was the interception of foreign intelligence signals and telephone communications from non-military parties such as governments, organizations, businesses and individuals. This program would come to be

---


31 NATIONAL SECURITY AGENCY, NSA/CSS MANUAL 22-1, at 7 (1986).


33 *Id.*
known as ECHELON and by some accounts, is currently active, intercepting e-mails, faxes, telefaxes, and telephone communications.34

ECHELON refers broadly to the global surveillance of communications intelligence between the United States and other nations.35 Although ECHELON has been described by historians and scholars as a specific computer network, other researchers write that the boundaries of the program are difficult to identify; therefore, ECHELON in this dissertation refers to the communications surveillance activities of the United States.36

The United States’ National Security Agency coordinates the ECHELON network to provide “global coverage” of COMINT, which includes telephone and telegraphic communications.37 This global coverage includes both signals collection and processing.38 One example of an ECHELON program is Operation Shamrock conducted in the mid-twentieth century. Developments in cellular and satellite communications have expanded ECHELON’s focus beyond traditional telephony. The ECHELON program has expanded to intercept Internet communications. In the mid 1990s, an NSA whistleblower claimed that the agency was monitoring Internet traffic at nine major exchanges where traffic was routed across United States borders.39 Although the advanced technological capabilities of the ECHELON network are


35 Lawrence D. Sloan, Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation, 50 DUKE L.J. 1467 (2001).

36 Id. at 1470.

37 Id. at 1471.

38 Id. at 1475.

39 Id. at 1478.
debated, there appears to be some sort of international cooperative agreement in place to collect and filter COMINT traffic using transnational supercomputers searching for key-word patterns.\(^{40}\)

The National Security Agency is a secretive organization. The number of employees and the allotted budget is not public record. The NSA website says that if it were considered a corporation in terms of “dollars spent, floor space occupied, and personnel employed” it would rank in the top 10 percent of Fortune 500 companies.\(^{41}\) The Office of Management and Budget, the Senate Select Committee on Intelligence, and the House of Representatives Permanent Select Committee on Intelligence, oversee the NSA’s classified budget.\(^{42}\) Figures are available for the overall U.S. government intelligence and related activities for 1997 and 1998.\(^{43}\) In 1997, the aggregate intelligence budget was 26.6 billion dollars; in 1998, the budget was 26.7 billion dollars.\(^{44}\)

The director of the NSA, who must be a commissioned officer with at least a three-star rank, is recommended by the U.S. Secretary of Defense and approved by the President.\(^{45}\)

---

\(^{40}\) See Kevin J. Lawner, *Post-Sept. 11th International Surveillance Activity—A Failure of Intelligence: The Echelon Interception System & The Fundamental Right To Privacy in Europe*, 14 PACE INT’L L. REV. 435 (2002). The European Parliament formed a temporary committee to investigate ECHELON and issued a report in 2001. The report found that there was “no longer… doubt” about the existence of the ECHELON program. The report states that the ECHELON program is being used to intercept private and commercial communications. The report also states that the system depends largely on the interception of satellite communications. *EUROPEAN PARLIAMENT, REPORT ON THE EXISTENCE OF A GLOBAL SYSTEM FOR THE INTERCEPTION OF PRIVATE AND COMMERCIAL COMMUNICATIONS (ECHELON INTERCEPTION SYSTEM)* 11 & 133 (July 11, 2001), available at http://cryptome.org/echelon-ep-fin.htm.


\(^{42}\) *Id.*

\(^{43}\) *Id.*

\(^{44}\) *Id.*

remaining NSA organization chart, like the budget, is classified by Public law 86-36. This law protects the NSA from having to release even unclassified organizational information. This law has protected many details of U.S. intelligence activities.

**Title III: Omnibus Crime Control and Safe Streets Act**

Despite the fact that the National Security Agency had been engaging in classified intelligence acquisition since the 1950’s, twenty years would pass before Congress first addressed government surveillance of private communications. In 1968, Title III of the Omnibus Crime Control and Safe Streets Act, adopted June 19, 1968 (hereinafter Omnibus Crime Act), gave the U.S. Attorney General the power to seek a warrant from a federal district court, or a federal court of appeals, to conduct electronic surveillance when investigating “particular” crimes. The law was, in part, a response to two U.S. Supreme Court decisions: 1) the 1967 *Berger v. New York* decision, outlining a statutory wiretapping scheme honoring Fourth Amendment criteria for search and seizure in cases of national security; and 2) the 1967 *Katz v.*

---


U.S. decision, which extended Fourth Amendment search and seizure protections to individuals, although it left open the legality of warrantless surveillance in cases of national security.\textsuperscript{49} The Omnibus Crime Act was not intended to limit the President’s constitutional powers,\textsuperscript{50} but rather delineate categories for warrantless surveillance, including: 1) protecting the nation against “actual or potential attack or other hostile acts of a foreign power”; 2) obtaining essential foreign intelligence information; 3) protecting national security information; 4) protecting against the overthrow of the government by force or “unlawful means”; or 5) protecting against “clear and present danger” to the government’s structure or existence.\textsuperscript{51}

Congress found, as stated in The Omnibus Crime Act, that “extensive” wiretapping of interstate and intrastate network facilities was carried out without “legal sanctions,” and “without the consent of any parties of the conversations.”\textsuperscript{52} The act articulated a need to “define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.”\textsuperscript{53} Congress acknowledged a need to enable law enforcement to intercept communications as evidence of criminal activity and to prevent crimes.\textsuperscript{54} Conversely, Congress recognized the need to “safeguard the privacy of innocent persons” by requiring judicial oversight and limiting categories or offenses subject to electronic surveillance.\textsuperscript{55}


\textsuperscript{51} Id. at § 2511(3).

\textsuperscript{52} Id. at § 801(a).

\textsuperscript{53} Id. at § 801(b).

\textsuperscript{54} Id. at § 801(c).

\textsuperscript{55} Id. at §801 (d).
The Omnibus Crime Act defined wire communication as

any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications.\footnote{Id. at § 2510(1).}

This updates the Communications Act’s definition by broadly defining communication instead of the specific “writing, signs, signals, pictures and sounds.” The definition still defines communication in terms of between points of origin and reception, but expands the original specification of “instrumentalities, facilities, apparatus and services,” to cover operation by common carriers operating facilities.\footnote{The Communications Act § 153(a), 47 U.S.C. § 151 (1934). In the Communications Act, wire communication is defined as “transmission of writing, signs, signals, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception of such transmission, including all instrumentalities, facilities, apparatus, and services (among other things, the receipt, forwarding, and delivery of communications) incidental to such transmission.”} These changes reflect technological advancements and telecommunication network development made in the 34 years between the Communication Act and the Omnibus Crime Act.

Additionally, several new terms relating to communication are defined. The Omnibus Crime Act defines oral communication as “any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.”\footnote{Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2000)), at § 2511(2).} Intercept is defined as “the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical, or other device.”\footnote{Id. at § 2511(4).} Electronic device is defined as “any device or apparatus which can be used to intercept a wire or oral communication,” not involving a telephonic or telegraphic instrument or

\footnote{Id. at § 2510(1).}

\footnote{The Communications Act § 153(a), 47 U.S.C. § 151 (1934). In the Communications Act, wire communication is defined as “transmission of writing, signs, signals, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception of such transmission, including all instrumentalities, facilities, apparatus, and services (among other things, the receipt, forwarding, and delivery of communications) incidental to such transmission.”}


\footnote{Id. at § 2511(4).}
This would include devices used to intercept communications over wire lines, not actual bugs placed in phones or intercepts made at telecommunication facilities such as central offices where calls are routed. Contents of wire or oral communication are defined as “information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.”

The Omnibus Crime Act makes it unlawful to “willfully” intercept, endeavor to intercept, or procure another person to intercept wire or oral communication. It is also unlawful to “willfully” disclose, or “endeavor” to disclose the contents of any wire or oral communication obtained illegally. It is lawful for communication carriers’ agents to intercept or disclose communication content when engaging in activities that are necessary to the “rendition of service” as long as monitoring is not random, except in cases of mechanical or quality control checks.

The Omnibus Crime Act makes it illegal to manufacture, assemble, possess or sell an electronic device for the purpose of “surreptitious” interception of wire or oral communication. The act prohibits the use of intercepted communications as evidence in court, except when lawfully obtained under warrant. It also specifies that the U.S. Attorney General, or his designee, must authorize a federal judge to grant an order for surveillance when there is evidence of 1) espionage; 2) riots; 3) illegal financial dealings by labor organizations; 4) murder; 5)

---

60 Id. at § 2511(5).
61 Id. at § 2511(8).
62 Id. at § 2511 (1)(a) & (b).
63 Id. at § 2511(1)(c) & (d).
64 Id. at § 2511 (2)(a).
65 Id. at § 2512 (1)(a) & (b).
66 Id. at § 2515.
kidnapping; 6) robbery; 7) extortion; 8) bribery of public officials or witnesses; 9) wagering; 10) obstruction of criminal investigations; 11) presidential assassinations, kidnapping or assault; 12) violence or threats directed at commerce; 13) violence or threats directed against interstate and foreign travel; 14) fraud; 15) drug trafficking; 16) extortion; or 17) conspiracy.67

The Omnibus Crime Act provides for disclosure of lawfully intercepted communications when 1) disclosing contents to another investigative agency or officer acting in the capacity of official duties; 2) giving testimony under oath or affirmation in any criminal court or grand jury proceeding; or 3) incidentally obtaining information when lawfully intercepting the contents of communication not related to the incidentally obtained information.68

The Omnibus Crime Act specifies that applications for orders authorizing interception must be made in writing, “with proper authority,” on oath or affirmation to a judge. Applications must also contain a “full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief than an order should be issued.”69 The applicant must also show that other investigative procedures have “been tried and failed,” or appear to be “too dangerous… or unlikely to succeed.”70 The time period of interception must be specified, as well as the identity of the interception target, the nature and location of the communications facilities, and a description of the type of communication sought.71

In cases of “emergency situations,” or “conspiratorial activities threatening the national security interests,” requiring interception before a court order can be obtained, an request for

67 Id. at § 2516(1)(a)-(g).
68 Id. at § 2517(1)-(5).
69 Id. at § 2518 (1) (a) & (b).
70 Id. at § 2518(1)(c).
71 Id. at § 2518 (1) (d) & (4).
authorization must be made within 48 hours of the time the interception occurred.\textsuperscript{72} The planned interception must be terminated if the order is denied.\textsuperscript{73}

**Church Committee**

The Omnibus Crime Act established federal requirements for judicial approval in obtaining wiretaps, but it did not address the issue of warrants in cases of national security, or the limitations on presidential powers when the President’s constitutional duty to protect the country intersected with intelligence gathering restrictions on the executive branch. In 1972, President Nixon’s authorization of illegal electronic surveillance was revealed in the Watergate scandal. The Watergate Complex, in Washington D.C., was the site of the offices for the Democratic National Committee. On June 17, 1972, five men were arrested and charged with attempted burglary of the complex and the DNC office. The men were also charged with attempting to intercept communications from the office of the DNC chairman, Larry O’Brien. The men, seven of whom were on the payroll of the Committee to Re-elect the President, were convicted of the crimes in January of 1973.\textsuperscript{74} In 1975, Senator Frank Church from Idaho headed the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities.\textsuperscript{75} The Committee was formed to investigate United States intelligence over the

\textsuperscript{72} *Id.* at § 2518 (7) (a) & (b).

\textsuperscript{73} *Id.* at § 2518 (8).


course of the 20th century. In response to the Watergate scandal—and general federal wiretapping activities during the 1960’s and 1970’s—the Church report noted that

At no time, however, were the Justice Department's standards and procedures ever applied to NSA's electronic monitoring system and its 'watch listing' of American citizens. From the early 1960's until 1973, NSA compiled a list of individuals and organizations, including 1200 American citizens and domestic groups, whose communications were segregated from the mass of communications intercepted by the Agency, transcribed, and frequently disseminated to other agencies for intelligence purposes.76

In 1975, in response to the Church Committee investigation, NSA Director Lt. General Lew Allen told the Pike Committee of the U.S. House of Representatives “Messages to and from American citizens have been picked up in the course of gathering intelligence.”77 After investigating the United States intelligence gathering, the Church Committee released fourteen reports including volume 5, The National Security Agency and Fourth Amendment rights.78

The Church Committee looked at three companies involved in the Operation Shamrock surveillance program during WWII: RCA Global, ITT World Communications and Western Union International.79 Although the original Church report did not discuss the nature of these companies involvement, the committee discovered a relevant file after it completed its original investigation.80 The file contained internal memorandums showing that the Army Signal Security Agency, a military precursor to the NSA, went to the three telecommunications companies in

76 Church Report. The Justice Department standards and procedures refer to the wiretapping requirements outlined in the Omnibus Crime Act.


78 CHURCH COMMITTEE FINAL REPORT, supra note 4, Vol. 5.

79 Id.

80 Snider, supra note 30.
August of 1945 and asked for cooperation.\textsuperscript{81} The government asked the companies to turn over copies of their telegraph messages to federal agents so the intercepts could be reviewed for information pertaining to national security. At the time, the companies were told Attorney General Tom Clark said the operation was “not illegal.”\textsuperscript{82} ITT World International was the only company that initially refused the request, but it acquiesced after learning that RCA and Western Union had agreed to cooperate with the government.\textsuperscript{83} Knowledge of the operation was limited to a few executives from each company.\textsuperscript{84}

In December 1947, the companies sought protection from anticipated prosecution related to the program.\textsuperscript{85} A meeting and assurances from Secretary of Defense James Forrestal satisfied that request.\textsuperscript{86} Forrestal said he spoke on behalf of the President when assuring the companies

\textsuperscript{81} Id.
\textsuperscript{82} Id.
\textsuperscript{83} Id.
\textsuperscript{84} Id.
\textsuperscript{85} Id.
\textsuperscript{86} Id.  Athan G. Theoharis, \textit{The Truman Administration and the Decline of Civil Liberties: The FBI's Success in Securing Authorization for a Preventive Detention Program}, 64 J. Am. Hist., No. 4, at 1010-30 (1978). In footnote 14, Theoharis discusses federal wiretapping under President Truman’s administration, in particular the surveillance of communist sympathizers. Theoharis documents Attorney General Tom C. Clark’s July 1946 letter to secure President Truman’s “assent to an expansion of FBI wiretapping authority by selectively quoting from a May 21, 1940 Franklin D. Roosevelt directive and implying that the request he submitted to Truman in 1946 was merely a reaffirmation of that directive.” Theoharis says that Clark’s letter “deleted a key sentence from Roosevelt’s directive and by so doing would permit wiretapping of ‘subversive activities.’” Theoharis writes that Clark used the same technique in an unsuccessful request on August 17, 1948 to obtain Truman’s permission for what would have been “the first formal presidential authorization of FBI investigations of dissident political activities.” In regards to Operation Shamrock, Theoharis said:

In contrast, while there is no record of direct presidential concurrence, in 1947 and 1949 Secretaries of Defense James Forrestal and Louis Johnson, claiming to speak for President Truman, directed the international telecommunications companies RCA and ITT illegally to intercept certain international messages. Stressing national defense needs, the secretaries assured company executives that by complying with this request their companies would not be subject to prosecution in the federal courts (for violating the law against such interception incorporated in Section 605 of the Federal Communications Act of 1934.
that their cooperation “was essential to the national interest and that they would not be subject to Federal prosecution.”87 Forrestal did add that “he could not bind his successors in office,” and perhaps this is why, in 1948, he unsuccessfully asked Congress to amend §605 of Communications Act of 1934 to clarify the legality of the companies’ cooperation.88 In 1949, the companies sought additional assurances from the new Secretary of Defense Louis Johnson.89 Forrestal’s successor said he spoke on behalf of the Attorney General and the President in granting the requested assurances to the company.90 The legality of the telecommunications companies participation in Operation Shamrock’s was established by the executive branch after the program concluded. One result of the Church Committee report was the passage of Foreign Intelligence Surveillance Act.91

**Foreign Intelligence Surveillance Act**

Congress passed the Foreign Intelligence Surveillance Act of 1978 (hereinafter FISA) two years after the Church Committee reports were released, investigating United States intelligence activities. 92 President Carter signed the Foreign Intelligence Surveillance Act into law on October 25, 1978. The act 1) legalized non-criminal electronic surveillance within the United States for the purpose of collecting foreign intelligence or counterintelligence; 2) defined and identified “foreign powers” and agents of “foreign powers” for the purpose of electronic

---


87 Snider, *supra* note 30.

88 *Id.*

89 *Id.*

90 *Id.*

91 *Id.*

surveillance; 3) required probable cause be shown for surveillance orders to be authorized; 4) provided procedures for review of surveillance applications, and 5) outlined circumstances for lawful surveillance.

Unless otherwise authorized by statute, FISA requires the federal government to obtain a warrant before spying on American citizens on American soil. FISA allows the President—through the Attorney General—to authorize warrantless surveillance inside the United States for up to one year for the purpose of gathering foreign intelligence information. The act creates judicial and congressional oversight for government surveillance activities of foreign targets. Periodic reports must be made to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence detailing the interception of communications of United States’ persons.

FISA created a Foreign Intelligence Surveillance Court of seven judges (for terms of one to seven years), appointed by the Chief Justice of the United States Supreme Court to hear applications and grant orders “approving electronic surveillance anywhere within the United States.”93 The act also established the Foreign Intelligence Court of Review to hear appeals from the FISA Court. The Chief Justice also was required to appoint three judges to terms of three, five and seven years to serve on a FISA review court known as the Foreign Intelligence Surveillance Act Court of Appeals.94 The Justice Department presents evidence to the court, however the proceedings and court findings are sealed.

Electronic surveillance is defined as:

1. the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known

93 Id. at §103(a).
94 Id. at §103(b).
United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

2. the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States;

3. the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the send and all intended recipients are located within the United States; or

4. the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.95

“Wire communication” means “any communication… carried by a wire, cable or other like connection furnished or operated by… a common carrier for the transmission of interstate or foreign communications.”96 The definition of “contents”—“a communication” including “information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication,” is unchanged from the Omnibus Crime Act.97

Applications for warrants must be made in writing under oath or affirmation by a federal official with the approval of the U.S. Attorney General.98 The application must identify 1) the

95 Id. at §101(f)(1)-(4).
96 Id. at §101(l).
97 Id. at §101(n).
98 Id. at §§104(a), 201(b) & 201(a)(3)(A)&(B). FISA restricts electronic surveillance only to that conducted according to the Attorney General’s certification, minimization procedures and Congressional oversight. Applications can only be authorized if the President—through written authorization—empowers the Attorney General to approve applications to a court for electronic surveillance of a foreign power or agent of a foreign power, as long as the surveillance does not involve the “acquisition of communication of any United States person.”
federal officer requesting a warrant; 2) the “identity, if known, or a description of the target of
the electronic surveillance”; 3) the fact that the target is a foreign power or agent thereof; 4) the
facilities or places to be monitored; 5) a statement of minimization procedures employed; 6) a
“detailed description of the nature of the information sought”; 7) the certification of the properly
designated executive branch official authorizing the warrant request; 8) a statement of
surveillance means and if physical intrusion is required; 9) a statement of facts concerning
previous applications made involving target, facilities or other specified places; 10) a statement
of the period of time surveillance will be conducted, and 11) the devices involved and
minimization procedures employed for each device.99

The Attorney General must certify to the FISA Court that there is no “substantial
likelihood” of a United States person’s communications being acquired during the
surveillance.100 A “U.S. person” is 1) a citizen of the United States, 2) an alien with permanent
lawful U.S. residence, 3) an unincorporated association with a substantial number of U.S.
citizens or aliens, or 4) a U.S. corporation.101 If a United States citizen is the target or party to
the surveillance, judicial authorization from the FISA Court must be obtained within 72 hours
after surveillance begins.

Minimization requirements must be met to decrease the likelihood of a United States’
person’s communications being intercepted during the surveillance.102 Minimization procedures,
in regards to electronic surveillance, include 1) “specific procedures” to “minimize the
acquisition and retention” and “prohibit the dissemination” of nonpublic information on United

99 Id. at §104(a)(1)-(11).
100 Id.
101 Id.
102 For a discussion of minimization requirements, see supra Ch. 1 (Literature Review).
States persons; 2) procedures to prevent identification of any United States person in handling foreign intelligence information; 3) retention and dissemination of information that a crime has or is about to be committed; 4) procedures to ensure no disclosure, dissemination or use of communication contents—to which a U.S. person is party for longer than 24 hours—unless a court order is obtained or the Attorney General determines the “information indicates a threat of death or serious bodily harm to any person.”\textsuperscript{103}

When an application is made, a judge must grant the request for electronic surveillance if the above criteria are met as long as the target is a foreign power or agent of a foreign power. “No United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States.”\textsuperscript{104}

The U.S. president, through the Attorney General, “may” authorize surveillance without a court order for the purpose of acquiring foreign intelligence information for “a period not to exceed fifteen calendar days following a declaration of war by the Congress.”\textsuperscript{105} “Foreign powers,” under FISA, are defined to include any foreign governments, factions of foreign governments and groups controlled by foreign governments. FISA does not apply to extra-territorial jurisdictions, but is triggered when foreign communications pass through United States telecommunication facilities and networks. Warrantless surveillance cannot be authorized to intercept communications from 1) groups engaged in international terrorism or activities; 2)\footnote{\textsuperscript{103} FISA, at § 101(h)(1)-(4). \textsuperscript{104} Id. at §105(a)(3)(A). \textsuperscript{105} The NSA’s United States Signals Intelligence Directive 18 strictly prohibits the interception or collection of information about ”. . . US persons, entities, corporations or organizations . . .” without explicit written legal permission from the Attorney General of the United States. \textit{Id. at} §111; NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE, UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE 18 (1980), available at http://cryptome.org/nsa-ussid18.htm.}

---

85
foreign-based political organizations not substantially composed of U.S. persons; or 3) entities that are directed and controlled by foreign governments. The FISA application must show “probable cause” that the surveillance target is a “foreign power” or “agent of a foreign power.”

Foreign intelligence information is defined as information that relates to the ability of the United States to defend against 1) “actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; 2) sabotage or international terrorism by a foreign power or an agent of a foreign power; 3) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.” The definition of “foreign intelligence” also encompasses “information” about a foreign power or foreign territory that relates to 1) the national defense or security of the United States; or 2) the conduct of the foreign affairs of the United States.

International terrorism includes activities that “involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State.” These activities are considered international terrorism when they intend to 1) intimidate or coerce a civilian population; 2) influence the policy of a government by intimidation or coercion; or 3) affect the conduct of a government by assassination or

---

106 Probable cause is “an apparent state of facts found to exist upon reasonable inquiry which would induce a reasonable, intelligent, and prudent person to believe, in civil cases, that a cause of action existed.” BLACK’S LAW DICTIONARY 1365 (4th ed. 1968).


108 Id. at §101(c)(2)(A)&(B).

109 Id. at §101(c)(1).
kidnapping. To be considered international terrorism, the activities must occur “totally outside the United States,” or they must “transcend national boundaries.”

Under FISA, surveillance is only permissible if 1) the Foreign Intelligence Surveillance Court authorizes an order for surveillance or 2) the Attorney General—in an emergency—authorizes the surveillance, while an application is made for Court authorization within 24 hours. FISA court authorization only applies to specific types of surveillance targets. The first is foreign powers including a foreign government, a representative of a foreign government, an employee of a foreign government, a faction of foreign government not substantially composed of United States persons, an entity controlled by a foreign government, or a group engaged in international terrorism. This also includes acquisition of the “contents of communications transmitted” between these types of targets, as long as there is “no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is party,” and minimization procedures are utilized. The second type of target allowed under FISA, is 1) an agent of a foreign power including non-U.S. persons who are officers or employees of a foreign power; 2) anyone who acts in support of a foreign power’s efforts to gather intelligence information on U.S. soil, or 3) anyone who knowingly engages in sabotage or international terrorism on behalf of a foreign power.

---

110 Id. at §101(c)(2)(A)&(B).
111 Id. at §101(c)(2)(C).
112 Id. at § 101(a)(1)-(6) & §102(a)(1).
113 Id. at § 102(a)(1)(A)(i),(B)&(C).
114 Id. at § 101(b)(1)-(2).
Evidence not lawfully obtained under FISA must be suppressed in court.\textsuperscript{115} This statutory requirement has not been modified in the thirty years since the passage of the act. In cases of “unintentional acquisition” the contents of the communication “shall” be destroyed “upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.”\textsuperscript{116} If electronic surveillance is employed during an emergency, and approval is not obtained from a judge after the fact, the judge “must” serve the target with notice of the application facts, the period of surveillance and the fact that information was not obtained.\textsuperscript{117}

The Attorney General “may” direct a “specified communication common carrier” to first “furnish all information, facilities, or technical assistance necessary to accomplish electronic surveillance” in a way that will protect secrecy and “produce a minimum of interference” with the common carrier’s service of its customers. Secondly, the Attorney General “may” direct a common carrier to maintain “any records concerning the surveillance or the aid furnished.”\textsuperscript{118} Carriers “shall” be compensated by the government at the “prevailing rate.”\textsuperscript{119}

United States agents, employees and officers, in the normal course of their official duties to conduct electronic surveillance, are “authorized” by FISA to test the capabilities of electronic equipment. Judicial consent is not required for testing periods up to 90 days, but Attorney General permission is required if the testing period exceeds this time period.\textsuperscript{120} The contents of

\textsuperscript{115} Id. at §105(g).
\textsuperscript{116} Id. at §105(i).
\textsuperscript{117} Id. at §105 (j).
\textsuperscript{118} Id. at §201(a)(4)(A) &(B).
\textsuperscript{119} Id.
\textsuperscript{120} Id. at §105(f)(1)(A)-(D).
any communication acquired in this manner must be “destroyed before or immediately upon completion of the test.” The same federal agents can use electronic surveillance to “determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance.”121 Electronic Surveillance also can be used to train intelligence personnel if the consent of the target is obtained, and contents are destroyed “as soon as reasonably possible.”122

Any person who engages in electronic surveillance “under color of law” or discloses or uses information obtained “under color of law,” is subject to financial penalty and imprisonment.123 An “aggrieved person,” who is not a foreign power or agent of a foreign power, who can show that they were the target of illegal surveillance can seek monetary damages.124

Communication common carriers are authorized to “provide information, facilities, or technical assistance to persons authorized by law to intercept wire or oral communications or to conduct electronic surveillance” as long as they are provided with 1) a court order or Attorney General certification that no warrant or court order is required by law.125 The carrier—and its officers, employees, or agents—shall not disclose the existence of “any interception or surveillance” except as legally required. Carriers violating the prohibition on disclosure “shall”

121 Id. at §105(f)(2).
122 Id. at §105(f)(3).
123 Id. at §109(a)-(d).
124 Id. at §110.
125 2 U.S.C. § 201 (a)).
be subject to civil damages, but no one can sue them for “providing information, facilities, or assistance” in compliance with FISA proceedings.\textsuperscript{126}

\textbf{Electronic Communications Privacy Act}

The Electronic Communications Privacy Act of 1986 (hereinafter ECP Act) amended the Omnibus Crime Control and Safe Streets Act. The ECP Act extended restrictions on unauthorized interception of oral, wire and electronic communications by the government to include electronic communications.\textsuperscript{127} The act also created new provisions for dealing with access to stored communications through pen registers and trap and trace devices.\textsuperscript{128} These updates prohibit communication service providers from “knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient.” This safeguards U.S. citizen’s communications, including computer-enhanced communications, from unauthorized government surveillance or third party interception. The EPC Act essentially updated FISA’s definition of communication to include

\begin{itemize}
  \item \textsuperscript{126} \textit{Id.}
  \item \textsuperscript{128} \textit{Id.} U.S.C. 206 § 3127(3) (2000) defines “pen register” as:
    \begin{itemize}
      \item a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.
    \end{itemize}
  \item U.S.C. 206 § 3127(4) (2000) defines “trap and trace device” as:
    \begin{itemize}
      \item a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication.
    \end{itemize}
\end{itemize}
“computer-enhanced communications,” such as e-mail, web searches and call data stored in electronic databases.

The Electronic Communication Privacy Act makes it unlawful to intentionally access a telecommunications facility through which electronic communication service is provided without authorization. Disclosure of any electronic communication contents to the public is illegal. The ECP Act restricts government access to stored communications or call-identifying information such as the phone number dialed. A search warrant is required for intercepting 1) the contents of wire or electronic communications in electronic storage 2) the contents of wire or electronic communications in a remote computing service 3) subscriber records or 4) subscriber service information. The ECP Act dictates that government must provide notice of the interception of a communication to the subscriber affected within at least 90 days.

The definition of “contents” of any wire, oral, or electronic communication include “any information concerning the substance, purport, or meaning of that communication.” This definition is identical to the definitions of contents from the Omnibus Crime Act and the Foreign Intelligence Surveillance Act. The ECP Act defined electronic communication for the first time. “Electronic communication” means “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.”

---

130 Id. at § 2702(a)(1).
131 Id. at § 2703(a)-(c)
132 Id. at §§ 2703(b)(1)(B)), 2705(a), 2705(a)(1)(B), 2705(a)(2)&(4).
133 Id. at § 2510(8).
134 Id. at. § 2510(12).
Electronic communication does not include “any” wire or oral communications, nor does it include communication made through a tone-only paging device. 135 Electronic communication service includes services to users providing “the ability to send or receive wire or electronic communications,” including “any transfer of signals, writings, images, sound, data or intelligence of any nature transmitted in whole or in party by a wire, radio, electromagnetic, photoelectric, or photooptical system.”136

The ECP Act allowed the FBI to use national security letters to compel providers to produce “subscriber information and toll billing records information, or electronic communication transactional records.”137 When a national security letter is used to compel records, evidence must be provided to show that the information sought is “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.”138

**CALEA**

The Communication Assistance for Law Enforcement Act of 1994 (hereinafter CALEA) mandates telecommunications companies to assist law enforcement in executing court authorized

---

135 Id. at § 2510(12).

136 Id. at § 2510(15).

137 Id. at § 2709. When a national security letter is used to compel records, evidence must be provided to show that the information sought is “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities...” See also Press Release, Federal Bureau of Investigations, Frequently Asked Questions: National Security Letters, [http://www.fbi.gov/pressrel/pressrel07/nsl_faqs030907.htm](http://www.fbi.gov/pressrel/pressrel07/nsl_faqs030907.htm) (last visited June 21, 2008). According to the FBI, a National Security Letter is “a letter request for information from a third party that is issued by the FBI or by other government agencies with authority to conduct national security investigations.” The FBI press release says the following types of “transaction records” can be obtained using a National Security Letter: subscriber information, toll billing records, Internet service provider login records, electronic communication transaction records, financial records, money transfers, credit records and other consumer identifying information.

Whereas FISA mandated communication carriers to cooperate with federal agents conducting authorized surveillance, CALEA required carriers to have surveillance-ready networks in place so the companies could comply with court orders for electronic surveillance and not delay intelligence investigations.\footnote{Commc’ns Assistance for Law Enforcement Act of 1994 (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994).}

CALEA’s purpose was to “require appropriate authorization to activate interception of communications or access to call-identifying information,” as well as to prevent “interception or access” without authorization.\footnote{Id. at §229(b) (1) (A)&(B).} The act defines call-identifying information as “‘dialing or signaling information,’ identifying the ‘origin, direction, destination, or termination’ of communication generated or received by a subscriber using “any” telecommunication carrier’s equipment, facility, or service.\footnote{Id. at §102(2).} CALEA also required communications carriers to maintain “secure and accurate records of any interception or access with or without such authorization.”\footnote{Id. at §229(b)(2).}

The act mandates telecommunication carriers assist federal law enforcement agencies by updating equipment, facilities and services to facilitate the interception of wire and electronic communications.\footnote{Id. at §103(a).} When the government has “lawful authorization,” carriers must “expeditiously” isolate and enable government interception of communications both “concurrently”—in real time as the transmissions are made—or after the fact “as may be acceptable to the government.”\footnote{Id. at §103 (a)(1).} Call-identifying information must also be provided to the...
government “pursuant to a court order.” However, the physical location of the subscriber’s telephone number “may” not be disclosed.\textsuperscript{146} The intercepted communications and call-identifying information must be delivered to the government in a format capable of being utilized by the government with respect to “procured” equipment, facilities and services outside the “premises of the carrier.”\textsuperscript{147} These transmissions to the government must be made “unobtrusively” and “with a minimum of interference with any subscriber’s telecommunications and service.”

FISA and the ECP mandated telecommunication carrier cooperation and specified criteria for obtaining warrants for surveillance. CALEA was the first law to forbid agents from interfering with communications in the process of intercepting target’s communication contents. Specifically, communication carriers must protect: 1) “the privacy and security” of communications and call-identifying information not authorized to be intercepted; and 2) information regarding the government’s interception of communications and access to call-identifying information.\textsuperscript{148}

Surveillance authorized under CALEA has many limitations. First, neither law enforcement agencies nor federal officers can require carriers to configure systems using specific designs for equipment, facilities, services or “features,” systems by specific manufacturers, or systems offered by specific providers of “telecommunications support services.”\textsuperscript{149} The restrictions on government access to networks do not apply to “information services,” “private

\textsuperscript{146} Id. at §103(a)(2)(A)&(B).

\textsuperscript{147} Id. at §103(a)(3).

\textsuperscript{148} Id. at §103(a)(4) (A)&(B).

\textsuperscript{149} Id. at §103(b)(1)(A) & (B).
networks” or systems used solely to interconnect telecommunications carriers.150

Telecommunications carriers are not responsible for “decrypting” communications or for the government’s ability to decrypt subscriber or customer transmissions, except when a carrier provides the encryption itself and “possesses the information necessary to decrypt the communication.”151 CALEA allows telecommunications companies to recover costs incurred in making modifications to “equipment, facilities or services” to facilitate government surveillance and interception.152

In “emergency or exigent circumstances,” carriers—at their own discretion—may allow “monitoring” at carrier premises if that is the “only means” the government can intercept or access the communications it is trying to obtain.153 These “circumstances” are defined as cases where any authorized law enforcement officer, “reasonably determines” that surveillance of wire, oral or electronic communication is “necessary in an emergency situation” involving 1) “immediate danger of death or serious physical injury to any person”; 2) “conspiratorial

150 Id. at §103(b)(2)(A) & (B). §102(6)(A), (B)(i)-(iii) and (C) defines information services as “the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications. This includes “a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities, electronic publishing, and electronic messaging services. It does not include “any capability for a telecommunications carrier’s internal management, control, or operation of its telecommunications network.” The FCC defines private network, for the purposes of CALEA as “organizations that provide facilities-based private broadband networks or intranets to enable their members to communicate with one another and/or retrieve information from shared data libraries not available to the general public.” See Federal Communications Commission, Communications Assistance for Law Enforcement Act and Broadband Access and Services Notice of Proposed Rulemaking and Declaratory Ruling, ET Docket No. 04-295 (Rel. Aug. 9, 2004), RM-10865, published 69 Fed. Reg. 56,976 (Sept. 23, 2005), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-04-187A1.pdf

151 CALEA, at §103(b)(3).

152 Id. at §103(e)(1).

153 Id. at §103(c).
activities threatening the national security interest”; or 3) “conspiratorial activities characteristic of organized crime.” \(^\text{154}\)

Even in this type of emergency circumstance, an order must be obtained within 48 hours after interception has occurred. \(^\text{155}\) If an order is nonexistent, then the interception shall immediately terminate when 1) “the communication sought is obtained” or 2) when the application for the order is denied.” \(^\text{156}\) In cases where surveillance is terminated without an order, the contents of interception must be “treated as having been obtained in violation of this chapter.” \(^\text{157}\) The contents intercepted would then be destroyed.

Applications for orders authorizing surveillance must be made in writing to a judge and must include the identities of the officers making and authorizing the interpretation. A full statement of the facts and circumstances relied upon, including the offense involved and the facilities and types of communications that will be intercepted must also be specified. \(^\text{158}\) With this information, a judge can make a temporary order authorizing surveillance of a facility within the court’s geographical jurisdiction. \(^\text{159}\) The judge can authorize surveillance outside the jurisdiction if an interception involves a mobile device and there is 1) probable cause a crime is about to be—or has been—committed; 2) the interception is likely to successful; 3) “normal investigative procedures” have failed, or appear likely to fail or “be too dangerous”; and 4) there is probable cause that telecommunication facilities specified will be used in connection with the

\(^{154}\) Id. at §2518 (7).

\(^{155}\) Id. at §2517(7)(b).

\(^{156}\) Id.

\(^{157}\) Id.

\(^{158}\) Id. at §2518(1)(a)&(b).

\(^{159}\) Id. at §2518(3).
offense. The four criteria do not have to be met if 1) the application for a warrant is made by a federal investigative or law enforcement officer and authorized by a specified Justice Department official; 2) the judge finds that an application’s specification of these criteria are not practical; 3) there is probable cause to believe that specification of a telecommunications facility would thwart the intended interception and 4) the order limits interception to a time period reasonably presumed to “proximate” the period a target will be using the communication instrument.

CALEA prohibits the disclosure of intercepted information to any person other than the participants of a “wire or radio” communication except 1) to a communication participant’s “addressee,” ”agent” or “attorney”; 2) to a person “employed or authorized to forward such communication to its intended destination”; or 3) in response to a court subpoena; or 4) at the demand of a federal official legally authorized to demand disclosure of an intercepted communication.

The Telecommunications Act of 1996

The purpose of the Telecommunications Act of 1996 (hereinafter Telecommunications Act) is “to promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies.” The act was intended to encourage competition for telecommunications service, telecommunication equipment, cable television, television broadcasting, radio, the Internet and other computer services.

160 Id.
161 Id. at §2518 (11)(a)&(b).
162 Id. at § 605(d)(1) defines agent as “any person or employee of a person.”
163 Id. at §605(a)(4). Ship masters are also allowed to receive this information for people who are serving under them. Section 605(d)(1) defines agent as “any person or employee of a person.”
For the purpose of the act, “telecommunications” is defined as “transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.” 165 “Telecommunications Carrier” is defined by the act to include “any provider of telecommunications services,” that will be treated as a common carrier while engaged in telecommunication services.166

The Telecommunications Act removed state restrictions on competition in local and long-distance telephone service and established universal service to subsidize telecommunications service to public institutions at reasonable prices. Under the Act, Telecommunication carriers are required 1) to interconnect “directly or indirectly” with the facilities and equipment of other telecommunications carriers and 2) to not install “network features, functions, or capabilities that do not comply with the guidelines and standards established pursuant” to the statute.167 Local exchange carriers must comply with specific requirements, including 1) telecommunications service must not be prohibited from resale to competing carriers; 2) telephone numbers must be portable “to the extent technically feasible”; 3) dialing parity must be provided to competing carriers and 4) physical rights of ways for installing telecommunication wires must be accessible to competitors.168

**USA PATRIOT Act**

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (hereinafter PATRIOT Act), amended FISA and expanding the government’s wiretapping powers, was passed in response to the 9/11 terrorist

---

165 *Id.* at § 3(48).
166 *Id.* at § 3(49).
168 *Id.* at § 251(b).
attacks.\textsuperscript{169} PATRIOT Act amendments permit collection of foreign intelligence information from U.S. citizens, whereas in the past this type of collection was only legal in the surveillance of non-U.S. citizens.\textsuperscript{170} Collection of foreign intelligence information on U.S. citizens is only legal when U.S. citizens are not engaged in First Amendment activities.\textsuperscript{171} The FISA “wall” separating foreign and domestic intelligence operations was changed, whereas now foreign intelligence information need only be a “significant purpose,” rather than a “primary purpose” in obtaining a warrant.\textsuperscript{172}

Section 201 of the PATRIOT Act amended section 2516(1) of Title 18 of the United States Code to add criminal violations relating to “chemical weapons” and “terrorism” to the types of crimes that qualify for wiretapping. Prior to this change, law enforcement agents were not allowed to seek wiretaps for these types of criminal investigations.\textsuperscript{173}

Section 203(b) of the PATRIOT Act amended section 2517 of Title 18 of the United States Code by permitting law enforcement officers to share “contents of wire, oral, or electronic communication” with federal officials, other than law enforcement officers, concerned with “law enforcement, intelligence, protective, immigration, national defense or national security” issues.\textsuperscript{174} The shared information can only be used in conjunction with conducting “that person’s official duties.” Section 203(b) was scheduled to sunset on December 31, 2005.\textsuperscript{175}


\textsuperscript{170} Id. at §203(b)(2)(B)(i)&(ii).

\textsuperscript{171} Id. at §214(a)(1).

\textsuperscript{172} Id. at §218.

\textsuperscript{173} Id. at §201(2) (amending §2516(1)(q)).

\textsuperscript{174} Id. at §203(b)(1) (amending §2517(6)&(19)).

\textsuperscript{175} Id. at §224.
The definition of foreign intelligence was amended to include “information, whether or not concerning a United States person, that relates to the ability of the United States to protect against 1) an actual or potential attack or other “grave hostile acts” of a foreign power or an agent of a foreign power; 2) sabotage or international terrorism by a foreign power or an agent of a foreign power; or 3) clandestine intelligence activities by an agent of a foreign power.”\textsuperscript{176} Foreign intelligence also includes information “whether or not concerning a United States person” relating to a foreign power or foreign territory in connection with 1) the national defense or the security of the United States; or 2) the conduct of the foreign affairs of the United States.\textsuperscript{177} Section 203(d) gives law enforcement authorities the ability to lawfully share foreign intelligence and counterintelligence information “obtained as part of a criminal investigation.”\textsuperscript{178} Pre-PATRIOT, law enforcement agencies faced legal obstacles in sharing information related to intelligence. Foreign intelligence information is defined in the same manner as it is redefined in section 203(b).\textsuperscript{179} Section 204 amends Section 2511(2)(f) of Title 18 of the United States Code to add electronic communication to the traditional types of communication—wire and oral—covered by the original code.\textsuperscript{180}

Section 206 permits the use of roving wiretaps in circumstances where the court considering the warrant application finds that specifying a single location for surveillance “may” have the effect of interfering with the investigation in cases where the target is changing.

\textsuperscript{176} Id. at §203(b)(2)(A)(B)&(C) (emphasis added to highlight change in definition).

\textsuperscript{177} Id. at §203(b)(2)(B)(i)&(ii). For definition of “United States person,” see supra notes 92-126. See also The Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458 § 6001 (2004). The 2004 “lone wolf” amendment, expanded the definition of “foreign power” to include parties not linked to foreign governments or terrorist groups.

\textsuperscript{178} Id. at §203(d)(1).

\textsuperscript{179} Id. at §203(2)(A)(i).

\textsuperscript{180} Id. at §204(1)&(2).
locations to try and evade surveillance.\textsuperscript{181} This allows agents to wiretap a person, instead of a single mode of communication. Section 207 extended the duration of FISA surveillance of non-United States persons, who are agents of a foreign power, to from 90 to 120 days.\textsuperscript{182} Physical searches are extended from 45 to 90 days, except in cases of foreign powers, where the period is extended to 120 days.\textsuperscript{183} Extension of a surveillance warrant for a period of one year may be granted with judicial approval.\textsuperscript{184} Section 209 allows federal investigators to more easily seize voice mail communications, using a less restrictive search warrant instead of a wiretapping warrant.\textsuperscript{185} Sections 206, 207 and 209 were scheduled to sunset on December 31, 2005.\textsuperscript{186}

Section 212 of the PATRIOT Act allows telecommunication carriers to voluntarily disclose customer call communications and records to government agents when “the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.”\textsuperscript{187} The provider can also voluntarily disclose this information to “a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any

\textsuperscript{181} \emph{Id.} at §206. A roving wiretap need not specify the target’s location in the warrant application. This allows law enforcement officials to track and intercept the communication contents of targets using cellular phones.

\textsuperscript{182} \emph{Id.} at §207(a)(1)(A)&(B).

\textsuperscript{183} \emph{Id.} at §207(2)(A)&(C). \S 1821(5) defines “physical search” as

\begin{quote}
any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant be required for law enforcement purposes.
\end{quote}

This does not include electronic surveillance or acquisition of foreign intelligence information from “international or foreign communications, or foreign intelligence activities.”

\textsuperscript{184} \emph{Id.} at §207(b)(1)(B).

\textsuperscript{185} \emph{Id.} at §209(1)(A)&(B), & (2)(A)-(C).

\textsuperscript{186} \emph{Id.} at §224.

\textsuperscript{187} \emph{Id.} at §212(a)(1)(A)(B)(i)-(iii)&(3).
person justifies disclosure of the information.”188 Previously under FISA—and then CALEA—the carriers would be forbidden from disclosing contents unless authorized by a court order. This amendment gave the telecommunications carriers the discretion to contact federal officials if they discover what might be illegal activities or information suggesting a threat to national security. Section 212 was scheduled to sunset on December 31, 2005.189

Section 218 changed the FISA wall so that foreign intelligence gathering need only be a “significant purpose” in obtaining the warrant, rather than a primary purpose.190 Section 225 provides immunity for carriers complying with a FISA wiretap request by the government.

No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act.191

Sections 218 and 225 were scheduled to sunset on December 31, 2005.192

Section 213 allows federal agents to delay the required notification of the subject of a warrant if the court authorizing the surveillance “finds reasonable cause to believe that providing immediate notification of the execution of a warrant may have an adverse result” on an investigation.193 This amendment assists law enforcement officials in cases where notifying the target might cause the target to change locations or use other methods of communication to evade interception or collection of evidence related to the criminal investigation. Section 214 of

188 Id. at §212.
189 Id. at §224.
190 Id. at §218.
191 Id. at §225(h).
192 Id. at §224.
193 Id. at §213(1).
the PATRIOT Act made it easier for law enforcement officials to obtain a warrant for a pen register or a trap and trace device in cases of international terrorism. As with criminal investigations, foreign terrorism investigations now only require evidence that the information sought relates to foreign intelligence. Pre-PATRIOT, the requirement was that evidence be provided demonstrating that the facilities to be monitored had been—or were about to be—used by a target not engaged in protected First Amendment activities.\textsuperscript{194} Section 214 was scheduled to sunset on December 31, 2005.\textsuperscript{195} Section 501 requires the Attorney General to report, on a semiannual basis, to the Permanent Select Committee on Intelligence of the House of Representatives and the Senate Select Committee on Intelligence, providing the total number of applications for surveillance orders approved, granted, modified, or denied.

\textbf{USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005}

The House and the Senate approved separate PATRIOT reauthorization acts, H.R. 3199 and S. 1389, in July of 2005.\textsuperscript{196} The Senate passed an additional bill, the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, S. 2271, to safeguard civil liberties not addressed in the original bills passed in 2005. The President signed the House bill and the second Senate bill on March 9, 2006.\textsuperscript{197}

The House bill, known as the USA PATRIOT Improvement and Reauthorization Act of 2005, and the original Senate bill, made 14 of PATRIOT’s 16 sunset provisions permanent, and extended the sunset for roving wiretaps (Section 206). The House bill extended the deadlines to

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{194} \textit{Id.} at §214(a)(1).
\item \textsuperscript{195} \textit{Id.} at §224.
\item \textsuperscript{196} USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. Nos. 109-177 & 109-178.
\item \textsuperscript{197} BRIAN T. YEH & CHARLES DOYLE, USA PATRIOT IMPROVEMENT AND REAUTHORIZATION ACT OF 2005: A LEGAL ANALYSIS, CONG. RES. REP. NO. RL33332, (Dec. 21, 2006).
\end{itemize}
\end{footnotesize}
December 31, 2015, while the Senate bill extended the deadline to December 31, 2009. A
conference report was prepared as a compromise.\textsuperscript{198} Although the House agreed to the
conference report, the Senate sought more protection for civil liberties, resulting in a
Congressional action to postpone PATRIOT’s expiration date until February 3, 2006 so
additional legislation could be considered. The USA PATRIOT ACT Additional Reauthorizing
Amendment Act of 2006 (S. 2271) was passed by the Senate on March 1, 2006, extending the
sunset deadlines to March 10, 2006.\textsuperscript{199}

The USA PATRIOT Improvement and Reauthorization Act of 2005 makes permanent
many of the sunset provisions built into the PATRIOT Act of 2001, including: 1) section 203(b)
regarding information sharing; 2) section 207 regarding the duration of wiretaps; 3) section 209
regarding the seizure of voice mail; 4) section 212 regarding emergency disclosures of
communications content or related records to authorities; 5) section 214 regarding pen registers;
6) section 218 regarding the FISA wall; and 7) section 225 providing telecommunications
carriers immunity when executing a FISA warrant.

Sections 206 (roving wiretaps) and Section 215 (business records) are not permanent and
sunset on December 31, 2009. Section 215 of the PATRIOT Act provides access to business
records by federal investigators through the use of national security letters. The Director of the
FBI, or his designee, can apply for orders to compel the production of “tangible things” such as
“books, records, papers, documents, and other items” for the investigatory purpose of protecting
“against international terrorism or clandestine intelligence activities,” as long as the basis for the
request is not the target’s First Amendment activities. The order must be justified by foreign


intelligence investigation purposes, but this cannot be disclosed in the order; nor can any person disclose the actual request by the FBI.

The 2005 PATRIOT Act amendment requires the Attorney General to include additional information in his semiannual report to Congress, including not just the number of requested and approved warrants for FISA-authorized surveillance, but also the number of requests “granted, modified, or denied for the production of library records, book sale records, firearm sale records, tax return records, educational records and medical records.”200 Additionally, Section 113 of the PATRIOT Act was amended by the 2005 PATRIOT Reauthorization Act to expand the types of offenses that trigger the authorization to obtain a court order for wire, oral or electronic wiretaps. The expanded list of crimes include activities relating to: 1) biological weapons; 2) violence at international airports; 3) nuclear and weapons of mass destruction threats; 4) explosive materials; 5) receiving terrorist military training; 6) terrorist attacks against mass transit; 7) arson within U.S. special maritime and territorial jurisdiction; 8) torture; 9) firearm attacks in federal facilities; 10) killing federal employees; 11) killing certain foreign officials; 12) conspiracy to commit violence overseas; 13) harboring terrorists; 14) assault on a flight crew member with a dangerous weapon; 15) certain weapons offenses aboard an aircraft; 16) aggravated identity theft; 17) “smurfing,” a money laundering technique involving a large monetary transaction that is separated into smaller transactions to evade federal reporting requirements on large transactions; and 18) criminal violations of certain provisions of the Sherman Antitrust Act.201

200 Id.
201 Id. at §103.
USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006

The USA PATRIOT Act Additional Reauthorization Act of 2006 amended FISA and other federal wiretapping statutes. The 2006 act further clarified the use of national security letters by federal intelligence investigators, and gave letter recipients under the right to petition a FISA judge to eliminate or modify the nondisclosure order. Section 3 of the act requires a judge to conduct an initial review of the order within 72 hours of the request by the recipient of the national security letter to remove the nondisclosure requirement. The judge must provide the recipient with a written statement justifying his or her decision to modify the nondisclosure order. The judge must evaluate the requested disclosure of the existence of a national security letter to determine if it would 1) endanger national security; 2) interfere with criminal, counterterrorism or counterintelligence investigations; 3) interfere with diplomatic relations; or 4) endanger the life or physical safety of a person. If the Attorney General, Deputy Attorney General, Assistant Attorney General or FBI Director certify the letter, then the judge reviewing the order must show the federal official’s decision to certify the letter was made in bad faith in order to eliminate the order. Section 4 of the 2006 PATRIOT Reauthorization Act states that recipients of national security letters are excused from having to give the government authorities the name of the attorney counseling them whether to comply with the national security letter.

Protect America Act

The Protect America Act of 2007 amended the Foreign Intelligence Surveillance Act by eliminating surveillance warrant requirements for foreign intelligence targets “reasonably

---

202 Id.

203 A petition to remove the nondisclosure requirements can only be done after one year from the date the order was issued. Id. at § 3 & 215, respectively.
believed” to be outside of the United States.\textsuperscript{204} The bill passed the Senate on August 3, 2007, and the House on August 4, 2007. President George Bush signed the bill into law on August 5, 2007. The law expired on February 17, 2008, due to a sunset clause.\textsuperscript{205}

The Protect America Act amended FISA to allow the Attorney General or the Director of National Intelligence to authorize foreign intelligence acquisition for “periods of up to one year” for targets “reasonably believed to be outside of the United States” if 1) “reasonable procedures” are in place; 2) a “significant purpose of the acquisition is to obtain foreign intelligence” and 3) “minimization procedures” are employed.\textsuperscript{206} Previously, under Section 207 of the 2001 PATRIOT Act, the duration of FISA surveillance of non-United States person, who are agents of a foreign power, was capped at 120 days. There must be proof that the acquisition involves foreign intelligence information obtained with the assistance of a communication service provider.

These circumstances must be supported by “written certification, under oath,” with an affidavit of an appropriate official in the national security field.\textsuperscript{207} Certification of triggering circumstances is not required in identification of the “specific facilities, places, premises, or property at which the acquisition of foreign intelligence information will be directed.”\textsuperscript{208} Authorized acquisitions may require the person with access to the information—the subject of the order—to 1) “immediately provide the Government with all information, facilities, and assistance necessary” to accomplish the acquisition, while protecting its secrecy and producing a


\textsuperscript{205} Id. at §6(c).

\textsuperscript{206} Id. at §2(105)(B)(a)(1)-(5). See also The USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). Minimization procedures are modified at §218.

\textsuperscript{207} Id. at §2(105)(B)(b).

\textsuperscript{208} Id. at §2(105)(B)(b).
minimum amount of interference with the services that the carrier is providing to the target and
2) maintain requested records using “security procedures” provided by the Attorney General or
Direction of National Intelligence.\(^{209}\) The government “shall” compensate the person providing
this information at the “prevailing rate.”\(^{210}\) If the person fails to comply with the requested
information, the Attorney General “may” seek court assistance.\(^{211}\) If the person still does not
comply, he or she can be found in contempt of the Court, unless he or she can successfully
challenge the legality of the directive by petition.\(^{212}\) No cause of action “shall” be brought
against a person “providing any information, facilities, or assistance in accordance with a
directive under this section.”\(^{213}\)

The Protect America Act requires the Attorney General to submit the location verification
procedures to the FISA Court for review within 120 days of passage.\(^{214}\) The court must approve
the procedures within 180 days of passage. Section 4 requires a semi-annual report to Congress
by the Attorney General on “acquisitions” during the previous six-month period.

**Current Congressional Actions**

Currently, Congress is considering revisions to the United States electronic surveillance
law, spurred by a national debate over immunity for telecommunication carriers that cooperated
with the government in executing the Terrorist Surveillance Program.\(^{215}\) This cooperation—and

\(^{209}\) *Id.* at §2(105)((B)(c)(1)&(2).

\(^{210}\) *Id.* at §2(105)((B)(f).

\(^{211}\) *Id.* at §2(105)((B)(g).

\(^{212}\) *Id.* at §2(105)((B)(h)&(i).

\(^{213}\) *Id.* at §2(105)((B)(l).

\(^{214}\) *Id.* at §3.

\(^{215}\) Anne Broache, *Congress may OK ‘compromise’ bill to derail spying lawsuits*, May 30, 2008,

The latest action by the House, the amendment to the Senate’s amendment of the bill would make significant changes to the Foreign Intelligence Surveillance Act and attempts to modernize the body of surveillance law. FISA would be amended to change procedures for acquiring communications of targets outside the United States by authorizing the Attorney General or Director of National intelligence to jointly authorize—for a period of up to one year—electronic surveillance of targets to acquire foreign intelligence information.\footnote{H.R. 3773, §702(a)(b)(c)&(d).} This authorization would be prohibited if the intention of targeting a person outside of the U.S. were to acquire the communications of a person believed to be inside the United States. The targeting must be done in a manner consistent with the Fourth Amendment.\footnote{Id. at § 702(b)(5).} The Director of National Intelligence also would need to establish a training program for the intelligence community, following guidelines established by the Attorney General. Targeting also would require the Attorney General or the Director of National Intelligence to certify that appropriate limitations and procedures were followed in conducting the surveillance.\footnote{Id. at § 702(f)(1).}
conducted under emergency circumstances without judicial authorization would need to be submitted for review to the FISC of review within seven days.  

The Attorney General and the Director of National Intelligence would be authorized to direct communication carriers to cooperate with the government surveillance requests by providing information, facilities and assistance, but at the same time maintaining security procedures.  

Certifications for targeting and minimization procedures would be submitted to the FISC of Review. The Attorney General and the Director of National Intelligence would be required to assess compliance with these procedures every six months and submit the results of the review to the FISC. Department of Justice Inspectors General also would be authorized to review the assessments. Additionally, the Attorney General would be required to make semiannual reports to the intelligence and judiciary committees on authorizations for surveillance.  

To conduct electronic surveillance on a U.S. person located outside of the United States, applications for targeting must be made by a federal officer and approved by the Attorney General. The application must be reviewed by the FISC of Review, which can authorize surveillance orders for ninety days with ninety-day renewals. The Attorney General can make an emergency authorization if he determines an emergency exists, he informs a judge of his

221 Id. at § 702(g)(1)(A)&(B).
222 Id. at § 702(h).
223 Id. at § 702(i).
224 Id. at § 702(i)(5).
225 Id. at § 702(l).
226 Id. at § 703(a).
227 Id. at § 703(b)(1)(J).
decision and applies for FISC authorization within seven days of authorizing surveillance.\textsuperscript{228} The section also allows for joint applications of targets where surveillance will be conducted concurrently both inside and outside of the United States.\textsuperscript{229}

The amendment would make FISA the sole means for conducting electronic surveillance on domestic communications.\textsuperscript{230} The Attorney General would be required to submit semiannual reports to the congressional intelligence committees with copies of FISC orders, including retroactively submitting orders for the five years preceding the passage of the bill.\textsuperscript{231} The Attorney General would be required to submit emergency authorizations for the use of pen registers or trap and trace devices to the FISC within seven days for review.\textsuperscript{232} Department of Justice Inspectors General, the Director of National Intelligence, the National Security Agency and any other agencies involved with the Terrorist Surveillance Program would be required to review the establishment, implementation, product and use of the intercepts made through the program, as well as provide a report to the intelligence and judiciary committees.\textsuperscript{233} Federal agents would be authorized to collect foreign intelligence information from targets—not substantially composed of U.S. persons—engaged in international proliferation of weapons of mass destruction.\textsuperscript{234}

\begin{thebibliography}{1}
\bibitem{228} \textit{Id.} at § 703(d)(1)(B).
\bibitem{229} \textit{Id.} at § 705(a)&(b).
\bibitem{230} Title VII §708(c)(2) is amended by § 102(a) of H.R. 3773.
\bibitem{231} H.R. 3773 at § 707(a)&(b).
\bibitem{232} \textit{Id.} at §§ 105(6)(e)(1)(D)(6)&(7)(i), 108.
\bibitem{233} \textit{Id.} at §§ 109&110.
\bibitem{234} \textit{Id.} at § 111(a)&(b).
\end{thebibliography}
A ten-year statute of limitations would be put into effect for offenses with financial and criminal penalties outlined under FISA.\textsuperscript{235} The government would be allowed to intervene in federal or state civil suits against any person complying with a request for surveillance cooperation by an intelligence agency.\textsuperscript{236} Parties in the suits would be allowed to submit evidence even if that evidence is subject to state secrets privilege.\textsuperscript{237} Specifically, the Attorney General is required to provide the court of jurisdiction in such suits (based on carrier assistance to the government between September 1, 2001 and January 17, 2007, under the Terrorist Surveillance Program) evidence of assistance requests or directives related to the charges in the case.\textsuperscript{238}

A Commission on Warrantless Electronic Surveillance Activities would be established, through the legislative branch, to report to the President and Congress on all intelligence collection programs and activities inside the United States or regarding U.S. persons in effect as of September 1, 2001.\textsuperscript{239} The Commission must protect national security in carrying out its duties and submit interim reports.\textsuperscript{240} The Commission would be terminated 60 days after its final report.\textsuperscript{241}

The proposed amendment to FISA does not prohibit intelligence agencies from conducting lawful surveillance necessary to 1) “prevent Osama bin Laden, al Qaeda, or any other terrorist or terrorist organization from attacking the United States, any U.S. person, or any U.S. ally; 2)

\textsuperscript{235} Id. at § 112.
\textsuperscript{236} Id. at § 802.
\textsuperscript{237} Id. at § 802(b).
\textsuperscript{238} Id. at § 802(e).
\textsuperscript{239} Id. at § 301(b)(1).
\textsuperscript{240} Id. at § 301(b)(2).
\textsuperscript{241} Id. at § 301(j).
ensure the safety and security of U.S. Armed Forces, or any other officer or employee of the
government involved in protecting U.S. national security; or 3) protect the United States, any
U.S. person, or any U.S. ally from threats posed by weapons of mass destruction or other threats
to national security.242

The bill is currently in conference committee to resolve the differences between the Senate
and House amendments.243

**International Law**

Beyond federal statutes protecting electronic surveillance, the United States is also party to
international treaties that protect the human right to privacy. The General Assembly of the
United Nations adopted the Universal Declaration of Human Rights (hereinafter, Declaration) on
December 10, 1948.244 The Declaration is meant to be a “common standard of achievement for
all peoples and all nations” and a way to “promote respect for these rights and freedoms.”245
The preamble of the Declaration says the “recognition of the inherent dignity and of the equal
and inalienable rights of all members of the human family is the foundation of freedom, justice
and peace in the world.”

---

242 *Id.* at § 406.

http://www.govtrack.us/congress/bill.xpd?bill=s110-2248. As of June 14, 2008, the bill is still pending committee
review.


June 14, 2008).
The Declaration has no legally binding authority, but is meant to be a standard for nations to adhere to in promoting not just individual human rights, but also “friendly relations between nations.”

Article 12 of the Universal Declaration of Human Rights says

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Two other international agreements very similar to the Universal Declaration of Human Rights Article 12 should be included when considering the Declaration. Article 17 of the International Covenant on Civil and Political Rights says "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.”

The International Telecommunications Convention (ITC) is the Geneva-based governing body of international telecommunications subsidiaries. Article 22 of the ITC says that members agree to protect the “secrecy of international correspondence.” The convention also says that members can turn correspondence over to authorities in order to ensure the execution of “internal laws” or “international conventions.” The ITC covers the internal laws of member states.

---

246 In 1998, Ramsey Clark said: “The United States government pays lip service to the Declaration, but its courts have consistently refused to enforce its provisions reasoning it is not a legally binding treaty, or contract, but only a declaration.” Ramsey Clark, Founder, International Action Center, Keynote Address at the Fiftieth Anniversary of the Universal Declaration of Human Rights (Dec. 2, 1998), available at http://www.thirdworldtraveler.com/Human_Rights/RCClark_50thAnnivUDHR.html. The Declaration is a component of binding international law. Playing on this concept, Ramsey said United States citizens should “stop their own governments from violating these definitions of human rights.” Ramsey addressed a conference in Baghdad with a primary focus on the human rights of Iraqi citizens impacted by international sanctions. Ramsey Clark was the keynote speaker, in Baghdad, Iraq on December 2, 1998, at a conference on the fiftieth anniversary of the signing of the Universal Declaration of Human Rights.

CHAPTER 3
FIRST AND FOURTH AMENDMENT COURT DECISIONS

In this chapter, the constitutional issues involving electronic surveillance will be explored by reviewing the relevant, seminal First Amendment and Fourth Amendment court decisions. The First Amendment decisions will be reviewed chronologically, following the development of the “clear and present danger” test, as it relates to the chilling effect of government suppression of free speech. Many of these cases involve political speech made by members of organizations assembling to oppose the United States government, so the review will also highlight cases where the court rule of free assembly under the First Amendment. The Fourth Amendment decisions involving electronic surveillance will also be reviewed chronologically building on the historic privacy opinions as they have developed over time with the courts. Specifically, cases will be reviewed that establish a right to privacy for electronic communications through the application of the traditional protections against government search and seizure. In both the First and Fourth Amendment sections of this chapter, the review will emphasize cases where the courts have suggested government restrictions on constitutional freedom create a chilling effect of activities protected under the First Amendment. The idea of “breathing space” for ideas to compete in the marketplace, which is closely tied to the chilling effect, as discussed in chapter one, will also be highlighted when the Court uses the concept in its reasoning. The concepts of “chilling effect” and “breathing space” are rarely the main issues in deciding U.S. Supreme Court decisions, but their continual use has led to a widely accepted judicial doctrine often mentioned in cases involving government surveillance of subversive citizens.

The First Amendment Decisions

The First Amendment is an important starting point in looking at constitutional protections for targets of electronic surveillance by the government. The First Amendment’s protections for
free speech can be endangered by federal statutes that do not adequately protect a target engaging in activities such as political expression. Statutes can also limit a target’s ability or desire to express opinions due to the fear they will face repercussions in response to communicating their ideas.

The First Amendment states that

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.¹

The First Amendment, a part of the United States Bill of Rights, was ratified in 1791. It guarantees fundamental civil liberties including protection against the establishment of religion and for the free exercise of religion, freedom of speech, and freedom of the press. It also guarantees a right of people to petition the government for redress of grievances and the right to assemble for the purposes of petition or communication on “national questions.”

Two First Amendment legal principles are directly relevant to the government’s electronic surveillance of citizen’s phone communications. The first is the “chilling effect” of laws that restrict the First Amendment right to free expression. This concept has been applied in cases controlling potentially subversive political views such as communism. The Court has found that citizens have a First Amendment right to engage in this kind of expression despite the possibility of related illegal activities. The second concept is one of the “breathing space” necessary to ensure free expression in the marketplace of ideas. Although breathing space has been traditionally applied to potentially false statements of the press in libel cases, the idea is applicable to surveillance in the sense in that it suggests that government should not be able to restrict true political speech in the marketplace of ideas.

¹ U.S. CONST. amend. I.
As discussed in chapter one, the marketplace of ideas model for freedom of expression relies upon citizens being free to express political opinions that enhance the democratic process by promoting discourse. When the government takes action to prevent this type of communication, it infringes upon the breathing space citizen’s need to develop their ideas without fear of retribution. As Alexander Meiklejohn suggested, the purpose of the First Amendment is to ensure that individuals can participate in the political decision making process.²

Government regulations that restrict free speech and political discourse “chill” citizen involvement in the democratic process.³ Frederick Schauer attributed the chilling effect to two legal principals: 1) laws are people-made rules and it is difficult to predict the outcome of their application and 2) the legal system is not perfect and errors in the legislative and judicial processes pose harm to individuals. First Amendment protections for free speech can promote the free flow of information, but government interference in the realm of free speech can undermine this critical exchange in the political process.⁴

Citizens have a need for privacy to ensure there is “breathing space” to develop autonomous ideas and express their opinions without government interference or societal pressure. Although these ideas might conflict with widely accepted societal views, they are vital for promoting exchange in the marketplace of ideas. Freedom of speech is a fundamental First Amendment right that has been upheld and shaped by a body of court cases, which include decisions relating to sedition and war protests. Freedom of assembly is closely related to


⁴ Id. at 691-92.
freedom of speech. Contemporary citizens often use telecommunication channels to discuss political and legal issues, as well as personal matters. Communication over telecommunication devices and lines enable a highly-mobile citizenry to engage in democratic dialogue with fellow citizens who might be located too far away geographically for face to face discussion. Although the freedom of religion, press and petition clauses could be relevant to a discussion of electronic surveillance and First Amendment rights, they will be downplayed in this discussion, in part because of the scope of the research. The analysis of First Amendment cases will focus on the free speech and free assembly clauses of the First Amendment.

Before looking at case law involving the government suppression of free speech and assembly, it is important to establish the historical climate of the era to which the case law traces its roots. This time period centers on the United States’ involvement in World War I. On June 15, 1917, Congress passed the Espionage Act of 1917. The law allowed the government to prosecute individuals who caused “insubordination, disloyalty, mutiny, or refusal of duty in the military or naval forces of the United States.” It also criminalized promoting the success of United States’ enemies. The Espionage Act said:

Whoever, when the United States is at war, shall willfully make or convey false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies and whoever, when the United States is at war, shall willfully cause or attempt to cause insubordination, disloyalty, mutiny, or refusal of duty, in the military or naval forces of the United States, or shall willfully obstruct the recruiting or enlistment service of the United States, to the injury of the service or of the United States, shall be punished by a fine of not more than $10,000 or imprisonment for not more than twenty years, or both.

6 Id.
7 Id. at §3.
At the time of the Act’s passage, many U.S. citizens feared that dissent at home during war-time could undermine a U.S. victory abroad. Less than a year later, the Espionage Act of 1917 was amended by the Sedition Act of 1918, criminalizing “disloyal” language against the government.\(^8\) Again, it was feared that dissent could harm national morale. Whereas the Espionage Act criminalized actions to undermine the U.S. war effort, the Sedition Act criminalized speech and publications that criticized the government. The Sedition Act made it a federal crime to

\[\text{willfully utter, print, write, or publish any disloyal, profane, scurrilous, or abusive language about the form of government of the United States, or the Constitution of the United States, or the military or naval forces of the United States, or the flag of the United States.}\]\(^9\)

The Sedition Act criminalized the advocacy, teaching, defense or suggestion of any word that would “support of favor the cause of any country with which the United States is at war.”

The Espionage Act of 1917 and the subsequent Sedition Act of 1918 led to large number of Supreme Court cases addressing the issue of government suppression of citizen speech and association under the First Amendment. These cases will be reviewed with a specific focus on the language that supports a judicial lineage for the “chilling effect” as it relates to the marketplace of ideas, clear and present danger, free association, political speech and breathing space.

Although a lot of significant precedence in Supreme Court opinions supports the concepts of the chilling effect and breathing space, support of these ideas began with a dissenting opinion in the 1919 case of *Abrams v. U.S.*\(^{10}\) The Supreme Court has long been concerned with

---


\(^9\) *Id.*

\(^{10}\) Abrams v. United States, 250 U.S. 616 (1919).
providing opportunities to criticize the government and openly discuss public issues, even when majority opinions upheld laws that restricted or punished speech. Following the passage of the Espionage Act of 1917 and the Sedition Act of 1918, the Supreme Court decided three cases that would create the “clear and present danger test,” the early standard for evaluating the necessity of government suppression of free expression. In March of 1919, the Court decided Schenck v. United States, Frohwerk v. United States and Debs v. United States.11 U.S. Supreme Court Justice Oliver Wendell Holmes wrote the unanimous decisions for each of the cases. In Schenck, the Court held that opposition to the Espionage Act was a “clear and present danger,” to the nation in general, and more specifically, the military.12

**Schenck v. United States**

In Schenck, for the first time the Supreme Court, in a 9-0 decision, upheld the constitutionality of the Espionage Act and therefore Charles Schenck’s conviction.13 Schenck was the secretary of the Socialist Party, which printed and distributed 15,000 leaflets by mail encouraging opposition to the military draft. The leaflets, in “impassioned language” described “military conscription” as the “worst form” of despotism and a “monstrous wrong against humanity.”14 Schenck was convicted on three counts: 1) conspiracy to violate the Espionage Act by causing and “attempting to cause” insubordination in the military and naval forces of the United States by obstructing the recruiting and enlistment effort, 2) conspiracy to commit and

---


12 *Schenck*, 249 U.S. at 52.

13 *Id.*

14 *Id.* at 51.
of offense against the United States, and 3) unlawful use of the mail for transmitting messages related to conspiracy against the United States.\textsuperscript{15}

The Court, in its decision, reasoned that Schenck did not deserve First Amendment protection when criticizing the draft because his action created a “clear and present danger” to the United States armed forces during a time of war. The Court reasoned that the intent of the Socialist Party’s document was to undermine the war effort because “the document would not have been sent unless it had been intended to have some effect, and we do not see what effect it could be expected to have upon persons subject to the draft except to influence them to obstruct the carrying of it out.”\textsuperscript{16} The Court acknowledged that during “ordinary times” the defendants would enjoy constitutional protection in distributing their leaflets during war times, the “character of every act depends upon the circumstances in which it is done.”\textsuperscript{17}

The Court, in the \textit{Schenck} decision, introduced one of the most famous clauses in First Amendment doctrine, “The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic.”\textsuperscript{18} Building on this idea, Holmes established the “clear and present danger test” that would become the new standard, at least until it was modified by later decisions, for government suppression of free expression:

\begin{quote}
The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent.\textsuperscript{19}
\end{quote}

\begin{flushleft}
\textsuperscript{15} \textit{Id}. at 49. \\
\textsuperscript{16} \textit{Id}. at 51. \\
\textsuperscript{17} \textit{Id}. at 52. \\
\textsuperscript{18} \textit{Id}. . \\
\textsuperscript{19} \textit{Id}. .
\end{flushleft}
The Court based its decision in *Schenck* on the question of “proximity and degree,” and said that words that enjoy tolerance during peacetime can be found to be unconstitutional during times of war.\(^{20}\) The Court reasoned that the purpose of the Espionage Act of 1917 was to punish “conspiracies to obstruct as well as actual obstruction.”\(^ {21}\) Therefore, the success of the conspiracy was not the measure of the crime.\(^ {22}\) Under the “clear and present danger” test, there were two tests for the protection of free speech. The first was based on circumstances, such as the nation being at war. The second was based on the intent of the speaker—whether or not he or she intended to bring about action against the government. In the second tier of the test, successfully executing the intent of a plan was not a necessary criteria in abridging the target’s speech. Mere intent to commit the type of crime barred by Congress was sufficient cause to secure a conviction.

In other words, in *Schenck*, the Court upheld acts specifically designed to curb or “chill” speech believed to be in conflict with national policy. Not surprisingly the First Amendment sensitive term “chilling effect” was not mentioned by name in the decision.

**Frohwerk v. United States**

A week after the *Schenck* decision, Holmes wrote the majority opinion in *Frohwerk v. United States*, repeating its support of the “clear and present danger” test.\(^ {23}\) In *Frohwerk*, the Supreme Court unanimously upheld the District Court of Western Missouri’s conviction of the defendant, Jacob Frohwerk for thirteen counts relating to the preparation and publication of anti-

\(^{20}\) Id.

\(^{21}\) Id.

\(^{22}\) Id.

\(^{23}\) Frohwerk v. United States, 249 U.S. 204 (1919).
draft articles. Frohwerk, a copy editor for a Missouri German language newspaper, had distributed twelve articles during 1917 promoting “disloyalty, mutiny and refusal of duty in the military and naval forces of the United States.” He was sentenced to ten years in prison, but he appealed on First Amendment grounds that his words were protected speech.

Relying on the Schenck decision, the Justice Holmes reasoned “the First Amendment, while prohibiting legislation against free speech as such, cannot have been, and obviously was not, intended to give immunity for every possible use of language.” Therefore, as in Schenck, “a person may be convicted of a conspiracy to obstruct recruiting by words of persuasion.” The Court decided the case on the standard in Schenck standard, determining if the publications were “overt acts” of conspiracy, rather than the on the basis the government asked for—Congress’ power “to punish such a conspiracy to obstruct.” The Court found little difference between the publications in Schenck and the publications currently being considered in Frohwerk.

The first expression by Frohwerk, referred to by the Court, was the declaration that it is “a monumental and inexcusable mistake to send our soldiers to France.” The publication referenced “the unconquerable spirit and undiminished strength of the German nation.” The paper called for an end to the war: "We say therefore, cease firing." Later, the publication said

---

24 Id. at 205.
25 Id.
26 Id.
27 Id. at 206.
28 Id. at 206-07.
29 Id. at 207.
30 Id.
31 Id.
32 Id.
that the “drafted man…recognizing that his country is not in danger and that he is being sent to a foreign land to fight in a cause that neither he nor any one else knows anything of, and reaching the conviction that this is but a war to protect some rich men’s money.”\textsuperscript{33}

Given this language, the Court reasoned that during times of war, although we do not “lose our right to condemn,” the “circulation of the paper was in quarters [neighborhoods] where a little breath would be enough to kindle a flame.”\textsuperscript{34} Although the publication was not specifically targeting men that might be drafted, it still had the potential to trigger reader opposition to the draft.\textsuperscript{35} The Court ruled that even though no means of conspiracy was specified, the publication still amounted to criminal conspiracy because Frohwerk intended “to accomplish” the goal.\textsuperscript{36}

As in \textit{Schenck}, the Court applied the new test of “clear and present danger,” requiring only intent to commit conspiracy—not a successful act to carry out a plan. Again, the decision, which does not use the term “chilling effect,” supported the idea that the government can chill “dangerous” speech that would otherwise be constitutionally protected speech. Words alone were sufficient to establish a threat under \textit{Frohwerk}. Instead of allowing potentially false or dangerous ideas to be tested in the marketplace, the Court upheld the government’s effort to stifle speech.

\textbf{Debs v. United States}

The last case of three decided in the Spring of 1919 was \textit{Debs v. United States}, involving the conviction of a former three-time Presidential candidate who had been spoken out against

\textsuperscript{33} \textit{Id.}
\textsuperscript{34} \textit{Id.} at 208-09.
\textsuperscript{35} \textit{Id.} at 209.
\textsuperscript{36} \textit{Id.}
World War II. Although the Court again did not mention the ‘clear and present danger’ test in its decision, it upheld the standard established in Schenck and Frohwerk.

On the same day it decided the Frohwerk case, the Supreme Court unanimously upheld the conviction of socialist political leader Eugene V. Debs under the Sedition Act of 1918, which amended the Espionage Act of 1917. The government said that Debs’ speech on June 16, 1918, in Canton, Ohio, was an attempt to “cause and incite insubordination, disloyalty, mutiny and refusal of duty in the military and naval forces of the United States.” In the speech, Debs praised a woman who was convicted of obstructing the enlistment service, in addition to honoring other people convicted the same crimes. He told those listening to him not to worry about the charge of treason leveled by the government if they joined the socialist cause, but instead “be concerned about the treason that involves yourselves.” Debs was convicted under the Espionage Act for opposing the official government war-time initiative by obstructing the recruitment and enlistment service of the United States military.

The Supreme Court, in its opinion, highlighted Deb’s sympathy for the persons honored in his speech against enlistment. The Court also highlighted a 1918 Socialist Party proclamation, “Anti-War Proclamation and Program,” endorsed by Debs. The proclamation declared that the war in Germany could not be justified, and that

---

38 Id.
39 Id. at 213.
40 Id. at 214.
41 Id. at 215.
We brand the declaration of war by our Governments as a crime against the people of the United States and against the nations of the world. In all modern history there has been no war more unjustifiable than the war in which we are about to engage.\(^{42}\)

The “clear and present danger” test was not mentioned in the opinion, and the intent of Deb’s words was not analyzed. Neither did the Court, again, mention the term “chilling effect.” Of course the decision, upholding a federal statute barring the advocacy of political change, could easily have “chilled” antiwar and other anti-government expression.

**Abrams v. United States**

The Court experienced an important turning point in the handling of free speech cases just eight months after it decided the trilogy of cases establishing and supporting the “clear and present danger” test. Most notably, *Abrams v. U.S.*, is not know so much for the majority’s decision—which supported the precedence of *Schenck, Frohwerk* and *Debs*—but rather the dissenting opinion of Justice Holmes. Holmes, the author of the opinions in *Schenck, Frohwerk* and *Debs*, broke with the majority in Abrams in what marked an important turning point in the judicial interpretation of “clear and present danger.”\(^{43}\)

In *Abrams*, decided in November 1919, the Supreme Court’s 7-2 majority upheld the conviction of the New York anarchists under the Espionage Act as constitutional. Jacob Abrams, Mollie Steimer, Hyman Lachowsky, and Samuel Lipman had participated in the publication of *Der Shturm*, a newspaper that advanced the anarchist political agenda in opposition to capitalism.\(^{44}\) The quartet, inspired by the Russian Revolution, dropped five thousand leaflets off of a rooftop in Manhattan advocating their anarchist cause.\(^{45}\) The leaflets

\(^{42}\) *Id.* at 215-16.

\(^{43}\) *Id.*

\(^{44}\) *Abrams v. United States*, 250 U.S. 616, 618 (1919).

\(^{45}\) *Id.* at 618.
were titled "Revolutionists Unite for Action," "The Hypocrisy of the United States and her Allies," and "Workers -- Wake up."\footnote{Id. at 618-19, 621.}

The men were arrested and convicted on October 25, 1918 in the United States District Court for the Southern District of New York on four counts. These included 1) “disloyal, scurrilous and abusive language about the form of Government of the United States,” 2) publication of language “intended to bring the form of Government of the United States into contempt, scorn, contumely and disrepute,” 3) publication of language “intended to incite, provoke and encourage resistance to the United States” in World War I, and 4) conspiring “when the United States was at war with the Imperial German Government, unlawfully and willfully, by utterance, writing, printing and publication, to urge, incite and advocate curtailment of production of things and products, to-wit, ordnance and ammunition, necessary and essential to the prosecution of the war.”\footnote{Id. at 621.} They were sentenced to prison for 15-20 year terms for advocating the overthrow of the United States government.

Before the Supreme Court, the government argued that the First Amendment did not apply to the New York anarchists because it was only meant to protect the press from prior government restraints on publication. Abrams and his associates were charged after the publication and distribution of their paper. The attorney for the journalists argued that the Espionage and Sedition Acts were an unconstitutional restraint on the men’s natural right of liberty of discussion.\footnote{Id. at 619.} Further, the attorney for the defendants in the case argued that the Espionage and Sedition Acts did not apply because the United States was not at war with the Soviet Union.\footnote{Id. at 618-19.}
Justice John Clark wrote the opinion of the Court, holding that the New York four were guilty of conspiring to violate the Espionage and Sedition Acts. The Court, relying on the clear and present danger test established in *Schenck*, reasoned that the government need only show that there was evidence of intent to overthrow the government. The Court said that the obvious purpose of the distributed papers was to “persuade the persons to whom it was addressed to turn a deaf ear to patriotic appeals in behalf of the Government of the United States, and to cease to render it assistance in the prosecution of the war.

The Court did not accept the claim that Abrams and his associates only intended to prevent United States involvement in the Russian Revolution, but rather through this “primary purpose,” their intent was to defeat the United States’ war effort. The Court emphasized that the four defendants were not seeking to bring about administrative change or “candid discussion” of the issue, but rather they were attempting to “defeat the war plans of the Government of the United States by bringing upon the country the paralysis of a general strike, thereby arresting the production of all munitions and other things essential to the conduct of the war.”

The Court used, as one example of the defendant’s intent to incite violence against the government, a pamphlet that read

> Do not let the Government scare you with their wild punishment in prisons, hanging and shooting. We must not and will not betray the splendid fighters of Russia. Workers, up to fight.

---

50 *Id.* at 617, 621.
51 *Id.* at 619.
52 *Id.* at 620-21.
53 *Id.* at 621.
54 *Id.* at 622.
55 *Id.* at 622.
The Court referred to another pamphlet to show that the defendants advocated revolutionary acts to “keep the armies of the allied countries busy at home.”\textsuperscript{56} The Court concluded that the pamphlets made clear the intent of Abrams and the others to “throw the country into a state of revolution.”\textsuperscript{57} Although the defendant’s “immediate occasion” for promoting the “outbreak of lawlessness” may have been to prevent sending troops to Russia, their actions could impede the United States war effort in Germany.\textsuperscript{58}

Justice Oliver Wendell Holmes, dissented from the majority opinion, joined by Justice Louis Brandeis. Holmes differed with the Court on the application of the “clear and present danger,” the test he originated in \textit{Schenck v. United States}. In his dissent, Holmes offered a revised test, one that he said afforded greater protection for political speech. Holmes’ new standard for the “clear and present danger” test, even though it was part of the \textit{Abrams} dissent, would become the standard for Supreme Court decisions on freedom of expression in the decades following \textit{Abrams}.

Holmes’ dissent said the four New York defendants posed no true threat to the United States’ war effort. Whereas previously the standard for clear and present danger was demonstrating there was a “present” danger to the government, Holmes in \textit{Abrams} specified that there must be proof of “imminent” danger. Holmes did not believe the words uttered by the four New York activists posed the same danger, or demonstrated an intent to harm the war effort, that the unrealized deeds they were advocating would.

\small\textsuperscript{56} Id. at 623.
\textsuperscript{57} Id.
\textsuperscript{58} Id.
Holmes argued that the sentiment in the pamphlets “in no way” was meant to attack the “form of government of the United States.” He based his new interpretation of intent, which he first established in the second tier of Schenck’s “clear and present danger” test, on the nature of Abrams’ words, which were not a specific act intended to overthrow the government, but rather an expression. Holmes said

But, when words are used exactly, a deed is not done with intent to produce a consequence unless that consequence is the aim of the deed. It may be obvious, and obvious to the actor, that the consequence will follow, and he may be liable for it even if he regrets it, but he does not do the act with intent to produce it unless the aim to produce it is the proximate motive of the specific act, although there may be some deeper motive behind.

Even though the words were uttered during a “time of war,” Holmes reasoned that the “principle of the right to free speech is always the same.” He argued that only a “present danger of immediate evil or an intent to bring it about” would warrant government intervention on expression. Holmes felt that “the surreptitious publishing of a silly leaflet by an unknown man” did not pose an “immediate danger” to the country. Furthermore, Holmes reasoned that there was no intent by the defendants other than helping Russia, and certainly there was no “hint at resistance to the United States” present in the defendant’s actions.

Holmes dedicated a large portion of his dissent to the discussion of “persecution for the expression of opinions.” He reasoned that sweeping away all opposition through suppression of speech was a “logical” action if the government did not want to face political dissent. He

59 Id. at 626.
60 Id. at 627.
61 Id. at 627-28.
62 Id. at 628.
63 Id.
64 Id. at 628-29.
65 Id. at 630.
write that under such an approach, allowing opposition indicates that the speech is impotent.\textsuperscript{66} Holmes said outlawing a class of speech indirectly acknowledges its power to reach the “ultimate good desired” by allowing “free trade in ideas.”\textsuperscript{67} In expanding on this “free trade in ideas,” Holmes used the marketplace of ideas metaphor for the first time in Court history to refer to the mechanics of free expression:

\begin{quote}
the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That, at any rate, is the theory of our Constitution. It is an experiment, as all life is an experiment. Every year, if not every day, we have to wager our salvation upon some prophecy based upon imperfect knowledge. While that experiment is part of our system, I think that we should be eternally vigilant against attempts to check the expression of opinions that we loathe and believe to be fraught with death, unless they so imminently threaten immediate interference with the lawful and pressing purposes of the law that an immediate check is required to save the country.\textsuperscript{68}
\end{quote}

In the Abrams case, the dissenting Justices said Schenck’s test of “danger” was not met. Although just two justices supported the dissenting opinion, its impact still echoes in modern theories of free expression. The Holmes-Brandeis dissent provided a conceptual rationale for free expression that is similar to the free market in economics on which the country is theoretically based.\textsuperscript{69} The Holmes-Brandeis dissent brought the advocacy of a free exchange of ideas by John Milton and John Stuart Mill into the 21\textsuperscript{st} century judicial ideology. For example, Holmes’ statement that “the best test of truth is the power of the thought to get itself accepted in the competition of the market” was reminiscent of Milton’s statement, “let her [truth] and falsehood

\begin{footnotes}
\item[66] Id.
\item[67] Id.
\item[68] Id. (emphasis added).
\end{footnotes}
grapple; who ever knew Truth put to the worse in a free and open encounter.”

Essentially, the Holmes-Brandeis dissent recognized the chilling effect of suppressing free expression in the democratic process.

**Gitlow v. New York**

The *Abrams* dissent of Holmes and Brandeis did not immediately change the Supreme Court’s pattern of affirming convictions based on speech or its reliance of the “clear and present danger” as developed in *Schenck*. In *Gitlow v. New York*, the Court upheld the defendants’ convictions under a New York criminal syndicalism statute. However, the *Gitlow* case is notable because the Court—for the first time—said that First Amendment protections ought to be extended to state government action against speech, in addition to federal suppression of speech.

In the 1925 case, *Gitlow v. New York*, decided by the U.S. Supreme Court in a 7-2 opinion, the Court upheld the conviction of a defendant under New York’s criminal anarchy law. The case was decided on the issue of whether the First Amendment’s free speech clause applied to states under the Fourteenth Amendment. Benjamin Gitlow and three conspirators were convicted of criminal anarchy under New York Penal Law, 160, 161.1. Gitlow was tried, convicted and sentenced separately, with the judgment affirmed by the Appellate Division and by the Court of Appeals of the state of New York.

---


71 Id. at 506.

The New York Statute defined “criminal anarchy” in section 160 as “the doctrine that organized government should be overthrown by force or violence, or by assassination of the executive head or of any of the executive officials of the government, or by an unlawful means.”

Furthermore, section 161§1 of the state criminalizes the advocacy of criminal anarchy by 1) word of mouth, 2) writing, 3) advising, or 4) teaching the duties of the doctrine. Section 161§2 criminalizes the actions made in section 161§1 when they are carried out through printing, publishing or editing issues related to criminal anarchy or knowingly circulating, selling, distributing, or displaying books, papers, documents or written printed matter relating to the doctrine.

**Gitlow** was convicted on two counts: 1) advocating, advising and teaching the doctrine of criminal anarchy through the writings in “The Left Wing Manifesto”, and 2) printing, publishing and circulating a paper titled, “The Revolutionary Age,” which advocated the forceful overthrow of government. The Court opinion specified “there was no evidence of any effect resulting from the publication and circulation of the Manifesto.”

The majority opinion was written by Justice Edward Terry Sanford, who was joined by Chief Justice William Howard Taft, and Justices Willis Van Devanter, James Clark McReynolds, George Sutherland and Harlan Fiske Stone. The Court upheld the New York statute criminalizing the advocacy of the overthrow of government by force or violence, but it simultaneously extended the Fourteenth Amendment’s due process clause to include the Bill of

---

133
The court clarified the “clear and present danger” test created in *Schenck* and expanded in *Abrams*.

In regards to the statute violating the Fourteenth Amendment’s protections, the Court said that while liberty of expression 'is not absolute,' it may be restrained 'only in circumstances where its exercise bears a causal relation with some substantive evil, consummated, attempted or likely,' and as the statute 'takes no account of circumstances,' it unduly restrains this liberty and is therefore unconstitutional.

However, the *Manifesto*, was found to advocate and urge “mass action which shall progressively foment industrial disturbances and through political mass strikes and revolutionary mass action overthrow and destroy organized parliamentary government.” The Court ruled that the language was not “the expression of philosophical abstraction,” but rather the “language of direct incitement.” The Court said that a State “may” punish utterance that endanger the foundations of organized government or “present a sufficient danger of substantive evil,” therefore Gitlow’s conviction must be upheld. Furthermore, the Court expanded on the clear and present danger test in saying that these types of utterances, by nature involve danger to the public peace and to the security of the State. They threaten breaches of the peace and ultimate revolution. And the immediate danger is none the less real and substantial, because the effect of a given utterance cannot be accurately foreseen. The State cannot reasonably be required to measure the danger from every such utterance in the nice balance of a jeweler’s scale. A single revolutionary spark may kindle a fire that, smouldering for a time, may burst into a sweeping and destructive conflagration. It cannot be said that the State is acting arbitrarily or unreasonably when in the exercise of its judgment as to the measures necessary to protect the public peace and safety, it seeks to extinguish the spark without waiting until it has enkindled the flame or blazed into the conflagration. It cannot reasonably be required to defer the adoption of measures for its

---

78 Previously, in *Barron v. Baltimore*, 32 U.S. 243 (1833), the Court held that the Bill of Rights only applied to the federal government.

79 *Gitlow*, 268 U.S. 652 at 664.

80 *Id.* at 665.

81 *Id.*

82 *Id.* at 667, 669.
own peace and safety until the revolutionary utterances lead to actual disturbances of the public peace or imminent and immediate danger of its own destruction; but it may, in the exercise of its judgment, suppress the threatened danger in its incipiency.  

The Court, relying on the reasoning in Schenck and Debs, specified that the defendant’s words did represent a “substantive evil,” and therefore created a “clear and present danger” to the nation.  

Again, since the statute was not “in itself unconstitutional,” the Court affirmed the Court of Appeals judgment.

Justice Holmes, who was joined by Brandeis, again dissented, arguing that the court should adhere to the “clear and present danger” standard for evidence establishing a substantive evil. Holmes and Brandeis, the justices respectively authoring and signing on to the dissent in Abrams, disagreed with the majority opinion in Gitlow. Holmes argued that Gitlow’s advocacy posed no present danger and only a few people would receive the message, with possible action taking place at an "indefinite time in the future."  

Relying upon Schenck, Holmes maintained that free speech must be extended protection under the Fourteenth Amendment. Holmes took issue with the majority labeling Gitlow’s manifesto as an “incitement,” writing that “every idea is an incitement” if it is believed.  

The only difference between the expression of an opinion and an incitement in the narrower sense is the speaker's enthusiasm for the result. Eloquence may set fire to reason. But whatever may be thought of the redundant discourse before us it had no chance of starting a present conflagration. If in the long run the beliefs expressed in proletarian dictatorship are destined to be accepted by the dominant forces of the community, the only meaning of free speech is that they should be given their chance and have their way.

---

83 Id. at 669.
84 Id. at 671.
85 Id.
86 Id. at 673.
87 Id.
88 Id. at 673.
Holmes and Brandeis, again, provided powerful language in *Gitlow*, which establishes the framework for a “chilling effect” of free speech at the hand of government action. Their handling of ideas conflicted with the majority’s reasoning that ideas alone could incite danger. Rather they suggested what could only be interpreted as a marketplace model: ideas “should be given their chance and have there way.” 89 This marketplace concept, which they first relied on in their *Abrams*’ dissent, is powerful support for the development of the “chilling effect” doctrine. Ideas must be allowed to compete in a market, free from government intervention that chills the natural discourse brought about by citizen exchange over true and false information.

**Whitney v. California**

In *Whitney v. California*, the Court did apply the “clear and present danger” test, sustaining a criminal conviction under the California Syndicalist statute.90 Brandeis and Holmes concurred in the opinion, again emphasizing that there was no evidence of “substantive evil” to create the danger needed to pass the Court’s adopted test.91 *Whitney* would remain the precedent for the “clear and present danger” test until it was overturned in 1969 by *Brandenburg v. Ohio*.

In *Whitney v. California*, decided May 16, 1927, the U.S. Supreme Court in a 9-0 vote, held that California’s criminal syndicalism law—criminalizing defense, advocacy or establishment of an organization committed to violent means of effecting government change—did not violate the First Amendment.92 The Superior Court of Alameda County, California convicted Charlotte Whitney under the California Criminal Syndicalism Act for helping to

89 Id.


91 Id.

92 Id. at 359-60.
establish the Communist Labor Party. Whitney was a member of the Oakland branch of the Socialist Party and she attended a convention in November of 1919 for the purpose of “organizing a California branch of the Communist Labor Party.” Whitney claimed that she had no intention of the party becoming an instrument of violent overthrow of the government. Whitney claimed she “took part in formulating and presenting” a convention resolution that would use legitimate political reform—the ballot—not acts criminalized by the California Syndicalism Act. The District Court of Appeals affirmed the judgment. Her petition to have the case heard by the Supreme Court was denied. Whitney brought appealed to the Supreme Court on writ of error, but the case was dismissed for “want of jurisdiction. The Court then granted a rehearing.

Justice Edward Sanford wrote the majority opinion. The Court held that the Syndicalism Act was “not repugnant to the due process clause by reason of vagueness and uncertainty of definition.” The Court said the Act “was not repugnant to the equal protection clause, on the ground that as its penalties are confined to those who advocate a resort to violent and unlawful methods as a means of changing industrial and political conditions.” The Court said the Act was also not “repugnant to the due process clause as a restraint of the rights of free speech,

---
93 Id. at 359.
94 Id. at 364.
95 Id. at 367-68.
96 Id. at 359 (citing People v. Whitney, 207 P. 698 (1922)).
97 Id. at 359.
98 Id. (citing People v. Whitney, 269 U.S. 530 (1925)).
99 Id.
100 Id. at 368.
101 Id. at 369.
assembly, and association,” because Constitutional freedom of speech does not confer an “absolute right to speak without responsibility.” The Court vacated the writ of error and affirmed the appeal court decision.

Justice Brandeis, joined by Justice Holmes wrote a concurring opinion. Brandeis said that the due process clause of the Fourteenth Amendment “applies to matters of substantive law as well as to matters of procedure,” therefore “all fundamental rights comprised within the term liberty are protected by the federal Constitution from invasion by the states.” He included free speech, the right to teach and the right of assembly as fundamental rights.

In regards to “clear and present danger,” Brandeis said the Court had not yet established a standard for establishing when danger is “clear,” or “how remote the danger may be and yet be deemed present.” He also insisted that the Court had not yet set a standard for how sufficiently substantial and evil must be to justify the abridgement of speech and assembly. Brandeis insisted an evil must be “substantial.”

Brandeis, in his concurring opinion, provide his interpretation of the Constitution framers’ intent behind guaranteeing liberty was the protection of political discussion as a fundamental principle of the American government:

They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth; that without free speech and assembly discussion would be futile; that with them, discussion affords ordinarily adequate protection against the dissemination of noxious doctrine.

102 Id. at 371.
103 Id. at 373.
104 Id. at 375-77.
105 Id. at 374.
106 Id.
107 Id. at 375-77.
Brandeis added that it was “hazardous to discourage thought, hope and imagination,” because it bred repression and prohibited “good” counsels from remediying “evil ones.”\(^\text{108}\)

Furthermore, he added that for free speech to be suppressed, there must be reasonable ground to believe that 1) evil will be a result of the speech, 2) the danger “apprehended” is imminent and 3) evil prevented is serious:

> Fear of serious injury cannot alone justify suppression of free speech and assembly. Men feared witches and burnt women. It is the function of speech to free men from the bondage of irrational fears.\(^\text{109}\)

He highlighted the difference between “advocacy and incitement,” “preparation and attempt,” and assembly and conspiracy as a difference “borne in mind.”\(^\text{110}\) He said that American should always be free to challenge the abridgement of speech unless an emergency justifies the government’s actions.\(^\text{111}\)

Brandeis said that “imminent danger” alone cannot justify the prohibition of free speech and assembly, there must be a “probability of serious injury to the state.”\(^\text{112}\) Brandeis concurrence is a departure from the majority views in Whitney, but it is an important turning point in First Amendment jurisprudence. In Abrams, Holmes argued that even unpopular ideas should be free to compete in the marketplace. Brandeis bolstered this argument in his Whitney concurrence by suggesting that free speech enabled the democratic process. His concurring opinion recommended changing the “clear and present danger” test to a time to answer test. Whereas the majority opinion indirectly embraced the governments need to chill violent

\(^{108}\) Id.

\(^{109}\) Id.

\(^{110}\) Id.

\(^{111}\) Id.

\(^{112}\) Id. at 377-78.
advocacy, Brandeis’ concurrence supported growing sentiment for his “marketplace” model introduced in Abrams. The Whitney concurrence would gain ground in the 1950’s and 1960’s as the Court decided free speech cases under the First Amendment. The marketplace model advocated by Brandeis in this concurring opinion, and preceding dissents with Holmes, would not find majority support in the Court until the 1969 Brandenburg v. Ohio decision overturned Whitney.\textsuperscript{113}

**Bridges v. California**

Fourteen years after the Whitney decision, the Court would issue an opinion that began to relax the application of the “clear and present danger” test. In Bridges v. California, decided December 8, 1941, the U.S. Supreme Court, in a 5-4 vote, held that the prior restrain of pretrial coverage by journalists was unconstitutional barring a “clear and present danger to the administration of justice.”\textsuperscript{114} The Court specified that the working principle of “clear and present danger” be based upon a ”substantive evil [that] must be extremely serious and the degree of imminence extremely high before high before utterances can be punished.”

The Bridges case was decided on appeal with the appeal of the Times-Mirror Co. v. Superior Court case.\textsuperscript{115} In Bridges, a union official, Harry Bridges, sent a telegram to the U.S. Secretary of Labor, threatening a strike if a judicial motion was enforced against unions. The letter was subsequently published in local California newspapers. The petitioners said the judicial motion was an abridgement of Constitutional protections for free speech and press. The

\textsuperscript{113} For a full discussion of Brandenburg v. Ohio, see infra.

\textsuperscript{114} Bridges v. California, 314 U.S. 252 (1941). Bridges was decided on appeal with a companion case, Times-Mirror Co. v. Superior Court, 310 U.S. 623 (1941).

\textsuperscript{115} In Times Mirror Co., the Los Angeles Times was convicted for contempt, when it published editorials on the sentencing of union members while a decision was pending. The decision was upheld by the lower appellate courts and the California Supreme Court.
lower appellate courts upheld his conviction for contempt of court. The Supreme Court sustained the First Amendment claims of the defendants and overturned both decisions on grounds that no “clear and present danger” had been shown. The Bridges case was decided on the issue of whether a publisher could be held in contempt of court for editorial statements made during a pending case.

The majority opinion was written by Justice Black, joined by Justices Hugo Black, William Douglas, Frank Murphy, Stanley Reed and Robert Jackson. The Court, relying on the reasoning in the Gitlow decision, held that punishment for an out of court publication, specifically being charged with contempt relating to a pending case, is only constitutional if the “clear and present danger” test can be met by showing a substantive evil that is likely to result from the utterances published.116 The degree of likelihood was a question pondered by the Court, as it relied on the Schenck “clear and present danger” test to evaluate whether the utterances were used in “such circumstances,” and of “such a nature,” that they would bring about a substantive evil.117

The Court said that the body of cases establishing the “clear and present danger” did not go to the outer limits of constitutional protections for expression, but rather recognized minimum protections under the Bill of Rights.118 The Court said that the First Amendment’s free speech and press clauses must be given as broad a scope as can be tolerated by society.119 An out of court publication, even if it has a “reasonable tendency” to interfere with the orderly

---

116 Bridges, 314 U.S. at 261, 263.
117 Id. at 261.
118 Id. at 263.
119 Id. at 265.
administration of justice, is not necessarily subject to punishment for contempt. The Court referred to the relevance of the “clear and present danger” test in cases of espionage, criminal syndication, anti-insurrection, breach of peace and substantive evils that could destroy or invade the right of privacy associated with life or property.

Nevertheless, the "clear and present danger" language of the Schenck case has afforded practical guidance in a great variety of cases in which the scope of constitutional protections of freedom of expression was in issue.

The Court said that in order to restrict free speech or press, an evil “must” be “substantial” and “serious.” The Court specified that “even the expression of ‘legislative preferences or beliefs’ cannot transform minor matters of public inconvenience or annoyance into substantive evils of sufficient weight to warrant the curtailment of liberty of expression.”

The working principle of the “clear and present danger” test is “that the substantive evil must be extremely serious, and the degree of imminence extremely high, before utterances can be punished.” The Court then analyzed the historical nature of the publications in the case—“publications tending to obstruct the orderly and fair administration of justice.” The Court concluded that the Constitutional framers intended the First Amendment to give “liberty of the press… the broadest scope that could be countenanced in an orderly society.” Furthermore,

---

120 Id. at 272.
122 Bridges, 314 U.S. at 262.
123 Id.
124 Id. at 262-63 (citing Schneider v. State, 308 U.S. 147, 161 (1939)).
125 Id. at 263.
126 Id.
127 Id. at 265.
the Court reasoned “Criteria applicable under the Constitution to other types of utterances are not applicable, in contempt proceedings, to out-of-court publications pertaining to a pending case.”

In regards to the publication at issue in the present case, the Court found that judgments below therefore produce their restrictive results at the precise time when public interest in the matters discussed would naturally be at its height. Moreover, the ban is likely to fall not only at a crucial time, but upon the most important topics of discussion. Here, for example, labor controversies were the topics of some of the publications. Experience shows that, the more acute labor controversies are, the more likely it is that, in some aspect, they will get into court. It is therefore the controversies that command most interest that the decisions below would remove from the arena of public discussion.

The Court held that the previous judgments in *Bridges* resulted in a curtailment of expression that cannot be dismissed as insignificant. If they can be justified at all, it must be in terms of some serious substantive evil which they are designed to avert.

Even though Bridges used the word “outrageous,” to describe the court’s handling of the labor dispute, there is no “threat” of “an illegal course of action.” Bridges, as Secretary of Labor, had an official duty to prevent strikes and was exercising the First Amendment right of petition in his duty as a United States government representative.

Where the majority opinion reversed the decisions of the lower courts, Justice Felix Frankfurter wrote the dissenting opinion, joined by Justices Harlan Stone, Owen Roberts, and

---

128 *Id.* at 268.
129 *Id.* at 268-69.
130 *Id.* at 270.
131 *Id.* at 277.
132 *Id.*
James Byrnes. Frankfurter saw the “administration of justice by an impartial judiciary” as basic to the concept of freedom, even when it was at odds with freedom of expression.  

Because freedom of public expression alone assures the unfolding of truth, it is indispensable to the democratic process. But even that freedom is not an absolute, and is not predetermined. By a doctrinaire overstatement of its scope, and by giving it an illusory absolute appearance, there is danger of thwarting the free choice and the responsibility of exercising it which are basic to a democratic society.  

Frankfurter argued that Bridges was attempting to “overawe” a judge and deprive the state of its powers to secure citizen justice. The dissenting opinion said that the majority opinion intimidated “the fair course of justice,” by allowing coercion of the courts.  

In Bridges, the Court’s opinion fell just short of rejecting the application of the “clear and present danger” test as it had been historically used in the cases leading up to and including Whitney. In modifying the “clear and present danger” test to require showing of “substantial” and “serious” harm, the Court began to embrace the line or reasoning in the Holmes and Brandeis dissents of the previous decades. This nod to the harm in chilling inconvenient or annoying speech, represented at least a temporary turning point, one where the Court began to recognize the need for citizens—even those with radical views—to be free to advocate courses of action, as long as they did not engage in specifically prohibited acts of overthrow or conspiracy.  

**West Virginia State Board of Education v. Barnette**  

The cases previously reviewed in this section focus clearly on the establishment and application of the “clear and present danger” test. Yet, the kinds of activities that triggered

---

133 *Id.* at 279.
134 *Id.* at 280-94.
135 *Id.* at 293.
136 *Id.* at 279.
137 *Id.* at 280.
prosecution under statutes prohibiting advocacy of government overthrow are closely related to another class of expression. In the early 1940’s the Court would be presented with an opportunity to rule on forced patriotism through a government mandate for symbolic speech. Although the case was closely tied to the First Amendment’ protection for religious freedom, the Court decided the case on the issue of free expression.

In *West Virginia State Board of Education v. Walter Barnette*, decided June 1943, the U.S. Supreme Court, in a 6-3 decision, held that the First Amendment’s establishment clause prohibits public schools from forcing students to salute the American flag and say the Pledge of Allegiance, affirming the lower district court decision. 138 The decision was significant because it overruled the Court’s 1940 decision in *Minersville School District v. Gobitis*, involving a plaintiff’s claim that his First Amendment right to free religion was abridged by a state compelling students to salute the American flag and recite the pledge. The majority opinion was written by Justice Robert Jackson, joined by Chief Justice Harlan Stone and Wiley Rutledge.139 Justices Black, Douglas and Murphy concurred with the opinion. The Court reasoned that compelling children to salute the flag and say the pledge of allegiance was a violation of the First and Fourteenth Amendments.140 Furthermore, compelled patriotism is not a permissible means of achieving “national unity.”141

Following the *Gobitis* decision, the West Virginia legislature had amended its statutes to require schools to “conduct courses of instruction in history, civics, and in the Constitutions of

---

139 Justices Hugo Black and William Douglas jointly concurred with the opinion, as did Justice Frank Murphy in a separate concurrence.
140 *Barnette*, 319 U.S at 637, 642.
141 Id. at 640.
the United States and of the State 'for the purpose of teaching, fostering and perpetuating the ideals, principles and spirit of Americanism, and increasing the knowledge of the organization and machinery of the government.'

On January 9, 1942, the Board of Education adopted a resolution, based on the *Gobitis* opinion, requiring the flag salute to become “a regular part of the program of activities in the public schools,” with all teachers and pupils being required to participate in the “salute honoring the Nation represented by the Flag; provided, however, that refusal to salute the Flag be regarded as an Act of insubordination, and shall be dealt with accordingly.”

The Parent and Teachers Association, The Boy and Girl Scouts, the Red Cross and the Federation of Women’s Clubs objected to the resolution as “being too much like Hitler’s.” Modifications were made so that only a “stiff-arm” salute were required, with the “right hand raised and palm turned up” while the pledge of allegiance was recited. If a child refused to salute the flag, he or she was expelled from school and denied readmission until they complied with the compelled salute. While expelled, they were considered truant from school and their parents were fined and faced jail time. The parents in the Barnette case, Jehovah’s Witnesses, brought suit against the Board of Education, arguing that the flag was an “image” that their religion forbade them from saluting in any manner. Therefore, a compelled salute was an “unconstitutional denial” of their religious freedom and freedom of speech, as well as the

---

142 *Id.* at 625 (citing Minersville Sch. Dist. v. Gobitis, 310 U.S. 586 (1940)).
143 *Id.* at 626.
144 *Id.* at 627.
145 *Id.*
146 *Id.* at 629.
147 *Id.* at 629-30. Exodus, Chapter 20, verses 4 and 5, says: “Thou shalt not make unto thee any graven image, or any likeness of anything that is in heaven above, or that is in the earth beneath, or that is in the water under the earth; thou shalt not bow down thyself to them nor serve them.”
Fourteenth Amendment’s due process and equal protection clauses. The District Court “restrained enforcement” of the compelled salute while the Board of Education appealed the case.

The U.S. Supreme Court identified the issue in the case as a conflict between authority and the rights of the individual, not an issue of religious freedom. Even though the Gobitis Court held that the State “may” require teaching in the history and structure of government—even to inspire patriotism and love of country—the compulsion of students to declare a belief goes beyond the Gobitis holding. The Court found that the flag salute—a form or utterance—was a “primitive but effective way of communicating ideas.” This “short cut from mind to mind” to “symbolize some system, idea, institution or personality” created loyalty among citizens, but failed to acknowledge that citizen’s do not garner meaning from compelled loyalty. The Court said that “A person gets from a symbol the meaning he puts into it, and what is one man's comfort and inspiration is another's jest and scorn.” Therefore, the Court reasoned that

148 Barnette, 319 U.S at 630. See also U.S. CONST. amend. XIV § 1:

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

149 Barnette, 319 U.S at 630.
150 Id.
151 Id. at 631.
152 Id.
153 Id. at 632.
154 Id. at 632-33.
“involuntary affirmation,” when commanded, violates the Bill of Rights safeguard for an individual to speak what is on his or her “own mind.”\textsuperscript{155}

It is now a commonplace that censorship or suppression of expression of opinion is tolerated by our Constitution only when the expression presents a clear and present danger of action of a kind the State is empowered to prevent and punish.\textsuperscript{156}

Not only would a compelled flag salute violate the protections guarded by the Bill of Rights, but since forced nationalism ignores an individual’s own beliefs, it is meaningless.\textsuperscript{157}

Any credo of nationalism is likely to include what some disapprove or to omit what others think essential, and to give off different overtones as it takes on different accents or interpretations. If official power exists to coerce acceptance of any patriotic creed, what it shall contain cannot be decided by courts, but must be largely discretionary with the ordaining authority, whose power to prescribe would no doubt include power to amend. Hence validity of the asserted power to force an American citizen publicly to profess any statement of belief or to engage in any ceremony of assent to one presents questions of power that must be considered independently of any idea we may have as to the utility of the ceremony in question.\textsuperscript{158}

The \textit{Gobitis} decision rejected a claim of religious freedom in favor of a need for national unity, but the \textit{Barnett} case is unique because, as the Court reasoned, “The question which underlies the flag salute controversy is whether such a ceremony so touching matters of opinion and political attitude may be imposed upon the individual by official authority under powers committed to any political organization under our Constitution.”\textsuperscript{159} The Court said the \textit{Gobitis} opinion found that “National unity is the basis of national security,” with authorities having the right to select the appropriate means for its attainment.\textsuperscript{160}

\begin{footnotes}
\item[155] \textit{Id.} at 634.
\item[156] \textit{Id.} at 624.
\item[157] \textit{Id.} at 625.
\item[158] \textit{Id.}
\item[159] \textit{Id.} at 635-36.
\item[160] \textit{Id.} at 640.
\end{footnotes}
Barnette, “National unity as an end which officials may foster by persuasion and example is not in question. The problem is whether under our Constitution compulsion as here employed is a permissible means for its achievement.” The Court felt it was not.

Struggles to coerce uniformity of sentiment in support of some end thought essential to their time and country have been waged by many good as well as by evil men. Nationalism is a relatively recent phenomenon but at other times and places the ends have been racial or territorial security, support of a dynasty or regime, and particular plans for saving souls. As first and moderate methods to attain unity have failed, those bent on its accomplishment must resort to an ever-increasing severity. As governmental pressure toward unity becomes greater, so strife becomes more bitter as to whose unity it shall be. Probably no deeper division of our people could proceed from any provocation than from finding it necessary to choose what doctrine and whose program public educational officials shall compel youth to unite in embracing.\(^{161}\)

The Court added that

those who begin coercive elimination of dissent soon find themselves exterminating dissenters. Compulsory unification of opinion achieves only the unanimity of the graveyard.\(^{162}\)

In regards to forced patriotism, the Court added that

freedom to differ is not limited to things that do not matter much. That would be a mere shadow of freedom. The test of its substance is the right to differ as to things that touch the heart of the existing order.\(^{163}\)

Additionally, the Court said that

If there is any fixed star in our constitutional constellation, it is that no official, high or petty, can prescribe what shall be orthodox in politics, nationalism, religion, or other matters of opinion or force citizens to confess by word or act their faith therein. If there are any circumstances which permit an exception, they do not now occur to us.\(^{164}\)

The Court’s decision in Barnett was significant because it addressed the underlying issue in the body of cases establishing the “clear and present danger” test. National unity was not a

---

\(^{161}\) Id. at 640-41.

\(^{162}\) Id. at 641.

\(^{163}\) Id. at 641-42.

\(^{164}\) Id. at 642.
goal that could be achieved by the government suppressing dissenting views for the sake of promoting the official United States policy. In mandating official government views, and compelling citizen adherence, the government was indirectly chilling the speech of citizens who objected to the policies. If citizens with opposing political views are silenced and their views criminalized through government actions, then they are robbed of the opportunity to participate in the marketplace of ideas. This undermines the democratic process revered in the United States. What is most important in the Barnett case is the language the Court used to describe compelled speech. It has direct relevance to the “chilling effect” doctrine, as it embraces a need for citizens to have “breathing space” to develop their ideas through political discourse.

**Dennis v. United States**

Although the U.S. Supreme Court traditionally sided with the government in the suppression of expression, the Bridges and Barnett cases represented a slight relaxation of the jurisprudence on patriotic ideals and the need to criminalize dissident speech. This departure would be short lived. In response to the communist scares of the 1940’s, Congress passed The Smith Act. The Smith Act, like the Espionage and Sedition Acts of the early 20th century, criminalized advocacy and intent to overthrow the government.

The Smith Act, passed in 1940, made it a felony to:

I. knowingly or willfully advocate, abet, advise, or teach the duty, necessity, desirability, or propriety of overthrowing or destroying any government in the United States by force or violence, or by the assassination of any officer of any such government;

---

165 Another First Amendment protection relevant to the Court’s decision in Barnett, is the right to protest war and the right to engage in political speech. See Cohen v. California, 403 U.S. 15 (1971) (upholding the right to wear a shirt which read, “Fuck the Draft”). The Supreme Court upheld a law prohibiting the destruction of draft cards in United States v. O’Brien in 1968. 391 U.S. 367 (1968). Although interfering with the draft was prohibited under the Smith Act, the Court upheld the right of students to protest the Vietnam War by wearing black armbands to school in Tinker v. Des Moines Independent Community School District. 393 U.S. 503 (1969). The Tinker holding would be weakened by the Bethel School District v. Fraser decision, which upheld a rule that punishing a student for speech in a public assembly. 478 U.S. 675 (1986).

II. with intent to cause the overthrow or destruction of any government in the United States, to print, publish, edit, issue, circulate, sell, distribute, or publicly display any written or printed matter advocating, advising, or teaching the duty, necessity, desirability, or propriety of overthrowing or destroying any government in the United States by force or violence;

III. to organize or help to organize any society, group, or assembly of persons who teach, advocate, or encourage the overthrow or destruction of any government in the United States by force or violence; or to be or become a member of, or affiliate with, any such society, group, or assembly of persons, knowing the purposes thereof.\textsuperscript{167}

The Smith Act also made it unlawful for “any person to attempt to commit, or to conspire to commit, any of the acts prohibited by the provisions of this title.”\textsuperscript{168} The Court would decide two important cases relating to the Smith Act: 1) \textit{Dennis} upholding the criminalization of advocacy of the overthrow of government and 2) \textit{Yates}, which barred the criminalization of mere advocacy and teaching of government overthrow. These opinions, though they updated the application of the “clear and present danger” test, did not depart from the Court’s previous decisions in \textit{Schenck}, \textit{Frohwerk}, \textit{Debs}, \textit{Abrams}, \textit{Whitney} and \textit{Gitlow}.

In \textit{Eugene Dennis, et al. v. United States}, decided June 4, 1951, the U.S. Supreme Court, in a 6-2 decision, affirmed the decision of the Second Circuit Court of Appeals and held that the defendants’ convictions for conspiracy to overthrow the government by force, by means of participation in the Communist Party, were not a violation of the First Amendment.\textsuperscript{169} The Petitioners were indicted in July of 1948, under the Smith Act.\textsuperscript{170} Petitioner Eugene Dennis was general secretary of the Communist Party of the United States.

\textsuperscript{167} Id. at 497. Section 2 (b) of the Smith Act states: “For the purposes of this section, the term ‘government in the United States’ means the Government of the United States, the government of any State, Territory, or possession of the United States, the government of the District of Columbia, or the government of any political subdivision of any of them.”

\textsuperscript{168} Smith Act, § 3.

\textsuperscript{169} Dennis v. United States, 341 U.S. 494 (1951).

\textsuperscript{170} Smith Act, 54 Stat. 671, 18 U.S.C. (1946 ed.).
The majority opinion was written by Chief Justice Fred Vinson, joined by Justices Stanley Reed, Harold Burton and Sherman Minton.171 The Court limited its review of the case to two questions: 1) Whether sections 2 and 3 of the Smith Act violate the First Amendment or any part of the Bill or Rights and 2) Whether Section 2 or 3 of the Act violate the First and Fifth Amendments because of “indefiniteness.”172 The Court chose not to consider whether the petitions did “in fact advocate the overthrow of the Government by force and violence,” but instead it would rely upon the affirmative decision of the Court of Appeals in this matter given the fact that it took six months to review evidence in the lower court case.173 Furthermore, on the issue of the petitioners’ intent with regards to their membership in the Communist Party, the Court wrote that intent to overthrow the government amounted to intent to deny others of constitutional rights.174

Since the purpose of the Smith Act was to “protect existing Government, not from change by peaceable, lawful and constitutional means, but from change by violence, revolution and terrorism,” Congress’ actions were not in conflict with constitutional protections for individuals.175 Since the “very language of the Smith Act” is directed at “advocacy, not discussion,” the Court found that “Congress did not intend to eradicate the free discussion of political theories, to destroy the traditional rights of Americans to discuss and evaluate ideas without fear of governmental sanction.”176 Congress intended to prevent action in the form of

---

171 Justices Felix Frankfurter and Robert Jackson concurred with the majority opinion. Justice Tom Clark did not take part in the decision.

172 Dennis, 341 U.S. at 495-96.

173 Id. at 497-98.

174 Id. at 500.

175 Id. at 501.

176 Id. at 501-02.
advocacy—the crime the petitioners were convicted of. It did not intend to limit their discussion of the issues.

Still, given the fact that the case was based on actions that contained an element of speech, the Court clarified the First Amendment issues arising out of the Smith Act’s enforcement.

the basis of the First Amendment is the hypothesis that speech can rebut speech, propaganda will answer propaganda, free debate of ideas will result in the wisest governmental policies. It is for this reason that this Court has recognized the inherent value of free discourse.\textsuperscript{177}

The Court added that freedom of speech is not unlimited—dissenters do not have “unlimited, unqualified” rights to speech—but rather speech must be weighed for its “societal value.”\textsuperscript{178} Based on previously decided cases, the Court deduced that “where an offense is specified by a statute in nonspeech or nonpress terms, a conviction relying upon speech or press as evidence of violation may be sustained only when the speech or publication created a "clear and present danger" of attempting or accomplishing the prohibited crime, e. g., interference with enlistment.”\textsuperscript{179} Specifically, the overthrow of government by force and violence “is certainly a substantial enough interest for the Government to limit speech. Indeed, this is the ultimate value of any society, for if a society cannot protect its very structure from armed internal attack, it must follow that no subordinate value can be protected.”\textsuperscript{180}

The Court said that the “literal problem” presented in \textit{Dennis} was the meaning of the phrase “clear and present danger.”\textsuperscript{181} The Court said that it did not mean the government has to

\textsuperscript{177} \textit{Id.} at 503.

\textsuperscript{178} \textit{Id.}

\textsuperscript{179} \textit{Id.} at 505.

\textsuperscript{180} \textit{Id.} at 509.

\textsuperscript{181} \textit{Id.}
wait for plans to be executed, it can intervene when it becomes aware of a plan involving overthrow.\footnote{Id.}

Certainly an attempt to overthrow the Government by force, even though doomed from the outset because of inadequate numbers of power of the revolutionists, is a sufficient evil for Congress to prevent. The damage which such attempts create both physically and politically to a nation makes it impossible to measure the validity in terms of the probability of success, or the immediacy of a successful attempt.\footnote{Id. at 510.}

The Court “rejected the contention that success or probability of success is the criterion “for clear and present danger.”\footnote{Id. at 510 (citing United States v. Dennis, 183 F.2d 201, 212 (2d Cir. 1950)).} The Court adopted a phrase from Chief Justice Learned Hand, “"In each case [courts] must ask whether the gravity of the `evil,' discounted by its improbability, justifies such invasion of free speech as is necessary to avoid the danger."\footnote{Id. at 510-11.} Just because the petitioners’ actions did not result in an attempt to overthrow the Government by force or violence, it does not mean that they are not guilty of advocacy.\footnote{Id. at 511.} The Court said that “It is the existence of the conspiracy which creates the danger…if the ingredients of the reaction are present, we cannot bind the Government to wait until the catalyst is added.”\footnote{Id. at 511.}

Justices Hugo Black and William Douglas dissented in separate opinions. In his dissenting opinion, Justice Black emphasized that the petitioners were not charged with attempt to overthrow the government, but rather they were charged because “they agreed to assemble and to talk and publish certain ideas at a later date,” as part of the Communist Party’s overall plan to
forcibly overthrow the government.  

Therefore, given The Smith Act’s enforcement as a prior restraint on speech and press, Black would find the law unconstitutional.  

Black said that the “clear and present danger” test was ignored in the majority opinion because of “expressed fear that advocacy of Communist doctrine endangers the safety of the Republic.”

Black argues that the judicial review of legislation “waters down” the First Amendment to a doctrine that protects only “safe” and “orthodox” views.  

In regards to the Communist scare, which prompted the passage of the Smith Act, Black wrote

> Public opinion being what it now is, few will protest the conviction of these Communist petitioners. There is hope, however, that in calmer times, when present pressures, passions and fears subside, this or some later Court will restore the First Amendment liberties to the high preferred place where they belong in a free society.

Douglas, in his dissenting opinion emphasized that the petitioners were convicted for merely teaching the Communist doctrine.  

They did not teach, in Douglas’s words, “the techniques of sabotage, the assassination of the President, the filching of documents from public files, the planting of bombs, the art of street warfare.”  

He says the preceding acts would not enjoy First Amendment protection, but “teaching” is “of a different character.”  

The petitioners organized people and themselves to learn the “Marxist-Leninist doctrine,” contained

---

188 Id. at 579.
189 Id.
190 Id. at 580.
191 Id.
192 Id. at 581.
193 Id. at 581-82.
194 Id. at 581.
195 Id. at 582.
in books. Douglas reasoned that since “the books themselves are not outlawed,” it cannot be a crime to teach the “creed” contained within them.

The crime then depends not on what is taught but on who the teacher is. That is to make freedom of speech turn not on what is said, but on the intent with which it is said. Once we start down that road we enter territory dangerous to the liberties of every citizen.

Douglas emphasized that the majority opinion made speech due “service for deeds,” essentially criminalizing speech.

The doctrine of conspiracy has served divers and oppressive purposes and in its broad reach can be made to do great evil. But never until today has anyone seriously thought that the ancient law of conspiracy could constitutionally be used to turn speech into seditious conduct.

Douglas argued that free speech is essential to democracy because it allows ideas to compete in the marketplace:

Free speech has occupied an exalted position because of the high service it has given our society. Its protection is essential to the very existence of a democracy. The airing of ideas releases pressures which otherwise might become destructive. When ideas compete in the market for acceptance, full and free discussion exposes the false and they gain few adherents. Full and free discussion even of ideas we hate encourages the testing of our own prejudices and preconceptions. Full and free discussion keeps a society from becoming stagnant and unprepared for the stresses and strains that work to tear all civilizations apart.

He adds that free speech—full and free discussion—is the foundation of our political system and the safeguard of “every religious, political, philosophical, economic, and racial group

196 Id.

So far as the present record is concerned, what petitioners did was to organize people to teach and themselves teach the Marxist-Leninist doctrine contained chiefly in four books: 3 Stalin, Foundations of Leninism (1924); Marx and Engels, Manifesto of the Communist Party (1848); Lenin, The State and Revolution (1917); History of the Communist Party of the Soviet Union (B.) (1939).

197 Id. at 583.

198 Id.

199 Id.

200 Id. at 584.
amongst us.”201 Douglas acknowledged, in deference to the “clear and present danger test,” that speech is dependant upon circumstances, but those circumstances only exist when “conditions are so critical that there will be no time to avoid the evil that the speech threatens.”202 He calls free speech the “strength of the nation,” and its “halt” the cause of the nation’s “destruction.”203 He adds that free speech is the rule, not the exception.204

Douglas concluded by adding that there is no evidence that Communism is gaining a stronghold in the United States, and therefore poses no “clear and present danger.”205 He describes Communism as a “bogeyman,” but “crippled as a political force” in the United States.206 He attributes this crippling to the positive effect of free speech and free discussion, with the American people “wanting none of it [communism].”207 Again, in regards to communism posing a “clear and present danger,” he says that the United States is “resilient” and the Communist “wares remain unsold.”208 In regards to the First Amendment, Douglas said that Congress should not be allowed to halt free speech, except in cases of “peril,” to the Nation.209 He added that the Court should have faith in the American people to “never give support to these

201 Id.
202 Id.
203 Id.
204 Id.
205 Id. at 588.
206 Id.
207 Id.
208 Id. at 588-89.
209 Id. at 590.
advocates of revolution, so long as we remain loyal to the purposes for which our Nation was founded.”

In *Dennis*, the majority opinion continued a tradition of judicial support for the government’s need to chill speech, which could potentially endanger the smooth functioning of the United States democratic process. The Court found that the government did not need to wait for a conspiracy to be successfully executed, it could intervene prior to the critical moment and prevent danger to the populous and the “Republic.” This, in some ways, amounts to a prior restraint on speech, in essence chilling speech believed harmful by the government. Black, in his dissent, acknowledged this prior restraint and found it to be an unconstitutional abridgment of free speech. Douglas, in his dissent, said that Communism should be free to compete in the marketplace of ideas because it was politically unviable and therefore, posed no “clear and present danger.” Though the majority opinion embraced the chilling effect, the dissenting opinions of Black and Douglas added weight to the theory of the chilling effect. The *Dennis* decision was followed six years later by the *Yates* decision, where the Court weakened the enforcement of the Smith Act, preventing prosecution for the advocacy of ideas alone.

**Yates v. United States**

In *Yates, et al. v. United States*, decided June 17, 1957, the U.S. Supreme Court, in a 6-1 decision, held that people must be encouraged to do something for there to be a violation of the Smith Act. Mere belief in an idea could not be criminalized. There must be advocacy for action to be taken. *Yates* involved the 1951 conviction of Oleta O’Connor Yates and 13 other petitioners charged under the Smith Act for being members of the Communist Party USA in

---

210 Id. at 591.

California. Yates claimed she was engaged in “passive actions” which were not forbidden under the Smith Act’s criminalization of “active” attempts to overthrow the government.

The Court found that evidence against five of the petitioners was insufficient for them to have been convicted by the lower court. The majority opinion was written by Justice John Marshall Harlan, II, joined by Chief Justice Earl Warrant and Justice Felix Frankfurter. Justice Harold Burton concurred. Justices Hugo Black and William Douglas concurred in part with the majority opinion. The Court reversed the convictions by the United States District Court for the Southern District of California and remanded the case to the District Court with instructions to acquit five of the petitioners and grant new trials to the remaining nine. The Court found the convictions, which rested upon the application of the Smith Act, were “hostile to the principles upon which its constitutionality was upheld” in the Dennis case. The 14 petitions were convicted of a single count of conspiracy made up of two parts 1) advocacy and teaching “the duty and necessity of overthrowing the Government of the United States by force and violence”; and 2) organization, as the Communist Party of the United States, of a “society of persons who so advocate and teach, all with the intent of causing the overthrow of the Government by force and violence as speedily as circumstances would permit.”

---


213 Yates, 354 U.S. at 327-34.

214 Id. at 300.

215 Id.
petitioners were each sentenced to five years and imprisonment and fined $10,000 each.\textsuperscript{216} The Court of appeals affirmed the decision, but the Supreme Court granted certiorari.\textsuperscript{217} 

The Court ruled that the indictment was not made under the Smith Act until 1951, six years after the Communist Party was founded in 1945. The statute of limitations for “organizing” an organization to overthrow the government was just three years.\textsuperscript{218} The word “organize,” as it was used in the Smith Act, was strictly construed by the Court to refer only to activities related to the creation of a new organization. The Court found the definition of “organize” did not relate to acts carried out after the formation of the organization.\textsuperscript{219}

The Court found that the Smith Act does not prohibit advocacy and teaching of forcible overthrow of Government, so long as it is taught as an abstract principle and not instigation to action.

Any advocacy or teaching which does not include the urging of force and violence as the means of overthrowing and destroying the Government of the United States is not within the issue of the indictment here, and can constitute no basis for any finding against the defendants.\textsuperscript{220}

The lower court had instructed the jury to convict if they found “advocacy,” to “incite” the forcible overthrow of the Government.\textsuperscript{221} The Court said that the First Amendment protected mere advocacy—“the true constitutional dividing line is not between inciting and abstract advocacy of forcible overthrow, but rather between advocacy as such, irrespective of its inciting

\textsuperscript{216} Id. at 302.
\textsuperscript{217} Id. at 303 (citing Yates v. United States, 225 F.2d 146 (9th Cir. 1955)).
\textsuperscript{218} Id. at 303.
\textsuperscript{219} Id. at 303, 304-12.
\textsuperscript{220} Id. at 314.
\textsuperscript{221} Id. at 312.
qualities, and the mere discussion or exposition of violent overthrow as an abstract theory.”222 The Court clarified that nothing in Dennis undermined the “distinction between the statement of an idea which may prompt its hearers to take unlawful action, and advocacy that such action be taken.”223 The Court said the interpretation of conspiracy under Dennis, was misinterpreted by the Court of Appeals in the Yates case, which mistakenly thought that proving an “overt act was an adequate substitute for the linking of the advocacy to the action which would otherwise have been necessary.”224 When the Appeals Court cited Dennis that “the existence of the conspiracy” creates the danger, they erred in interpreting the decision.225

Justice Burton concurred with the Court; except for its interpretation of the word “organize,” as used in the Smith Act.226 Justices Brennan and Whittaker took no part in the consideration or decision of the case. Justices Black and Douglas concurred in part and dissented in part.

Referencing his dissent with Justice Douglas in Dennis, Black wrote that he would “reverse every one of these convictions,” and acquit the defendants because the Smith Act unconstitutionally abridged the “freedom of speech, press and assembly.”227 Black said that the trials conducted in response to Smith Act convictions were “prolonged affairs lasting for months,” due to “massive collections” of evidence unmanageable by jurors.228 Black agreed with the majority’s definition of “organize,” and its holding that the trial judge erred in

222 Id. at 312-14.
223 Id. at 322.
224 Id.
225 Id. at 323 (citing Dennis, 341 U.S. at 510-11).
226 Id. at 338.
227 Id. at 339 (Black, J., concurring in part and dissenting in part).
228 Id.
instructing the jury about advocacy as an abstract principle under the Smith Act.\textsuperscript{229} He also agreed with the acquittal of five petitioners, although he thought all of the petitioners should be acquitted.\textsuperscript{230} Black said that he believes the “First Amendment forbids Congress to punish people for talking about public affairs, whether or not such discussion incites to action, legal or illegal.”\textsuperscript{231} Whereas, the Court held that attendance at Communist Party meetings constituted “overt action,” under the Smith Act, Black thought there was not enough evidence to convict since Article III§3 of the Constitution requires the testimony of two witnesses to the “same overt act” or a “confession in open court.”\textsuperscript{232} Black said this was an important protection because it kept people from “being convicted of disloyalty to government during periods of excitement, when passions and prejudices ran high, merely because they expressed unacceptable views.”\textsuperscript{233} Black says the defendants committed no “overt act” beyond attendance at a “constitutionally protected public assembly where they took part in lawful discussion of public questions, and where neither they nor anyone else advocated or suggested overthrow of the United States Government.”\textsuperscript{234}

Black felt the prosecution under the line of reasoning currently promoted encouraged an evolution towards “authoritarian government in which voices criticizing the existing order are summarily silenced.”\textsuperscript{235} He added, “Doubtlessly, dictators have to stamp out causes and beliefs

\textsuperscript{229} \textit{Id.} at 341.
\textsuperscript{230} \textit{Id.}
\textsuperscript{231} \textit{Id.}
\textsuperscript{232} \textit{Id.} at 342-43.
\textsuperscript{233} \textit{Id.} at 343 (citing Cramer v. United States, 325 U. S. 1 (1945)).
\textsuperscript{234} \textit{Id.}
\textsuperscript{235} \textit{Id.}
which they deem subversive to their evil regimes.” He concluded by discussing the Constitutional framers intent behind the First Amendment:

The choice expressed in the First Amendment in favor of free expression was made against a turbulent background by men such as Jefferson, Madison, and Mason -- men who believed that loyalty to the provisions of this Amendment was the best way to assure a long life for this new nation and its Government. Unless there is complete freedom for expression of all ideas, whether we like them or not, concerning the way government should be run and who shall run it, I doubt if any views, in the long run, can be secured against the censor. The First Amendment provides the only kind of security system that can preserve a free government -- one that leaves the way wide open for people to favor, discuss, advocate, or incite causes and doctrines however obnoxious and antagonistic such views may be to the rest of us.

Justice Clark, in his dissent, pointed out that the petitioners convicted under the Smith Act in the present case were “engaged in conspiracy with the defendants” in the Dennis case, although he acknowledges they were in a “lower echelon in the party hierarchy.” Therefore, Clark would affirm the convictions.

The majority opinion in Yates, protected the advocacy of “abstract principles” from government suppression. This was a significant shift from its decision in the Dennis case. Black, in his dissent, emphasized how free expression and assembly must be protected during periods of nation political “excitement.” Black, who saw the Smith Act as a prior restraint in Dennis, argued that citizens must be free to participate in constitutionally protected assemblies for the purpose of discussing matters important to their participation in the national governance process. Both the majority opinion, and Black’s dissent, supports the development of the “chilling effect” as an offshoot of the marketplace of ideas model. Abstract principles—or quite

236 Id.
237 Id. at 344.
238 Id. at 344-45.
239 Id. at 345.
simply, ideas—are best left to compete in the market for viability. When the government restricts their introduction to the market, it can interfere with an important political process that ensures citizens enjoy constitutionally guaranteed liberties.

**New York Times v. Sullivan**

The next case relevant to this review is a libel case, but it is relevant to a discussion of the marketplace of ideas as the Court struck down an Alabama law abridging freedom of expression under the First Amendment. More importantly, the Court makes use of the term “breathing space” to discuss the insular needs of the marketplace of ideas.

In *New York Times Co. v. L.B. Sullivan*, decided March 9, 1964, the U.S. Supreme Court, in a 9-0 decision, held that an Alabama libel law unconstitutionally abridged the petitioner’s freedom of speech and press guaranteed by the First Amendment. The First Amendment, applied through the Fourteenth Amendment’s due process clause, protected a newspaper from being sued for libel for making false defamatory statements about the official conduct of a public official, as long as the statements were not made with knowing or reckless disregard for the truth. The Court reversed the lower court decision and remanded the case.

The *New York Times*, on March 29, 1960, published full-page advertisement titled, “Heed Their Rising Voices.” The ad solicited funds to defend Martin Luther King, Jr. on an Alabama tax evasion charge. The ad also described police actions, including actions by the Montgomery, Alabama, police force against civil rights protestors. Montgomery City Commissioner L.B. Sullivan, who was one of three police department supervisors, was not named in the ad, but he interpreted the charges against the police department as defamation against him. The Ad

---


241 Id. at 265-92.
mentioned sixty-four persons by name. Sullivan, following Alabama libel law’s legal requirement that punitive damages could only sought if a written demand for public retraction failed or was refused, sent a request that the *Times* denied. Sullivan filed suit against the *Times*. Sullivan also successfully sued Ralph Abernathy, S.S. Seay, Sr., Fred Shuttlesworth and Joseph Lowery—the four black ministers mentioned in the ad—for $500,000 in Alabama Court.242

Justice William Brennan wrote the majority opinion, joined by Chief Justice Earl Warren and Justices Tom Clark, John Harlan, Potter Stewart, and Byron White. Justices Hugo Black and Arthur Goldberg each wrote separate concurrences, both joined by Justice William O. Douglas. The majority established a standard for “actual malice” in cases where press reports could be considered defamation and/or libel.243 To establish “actual malice,” a plaintiff must prove that the publisher of the statement in question knew that the statement was false or acted in reckless disregard of its truth or falsity.244

In the opinion, the Court introduced the need for “breathing space” as a condition for free debate and expression in society. Even erroneous statements in regards to political conduct and views need to be protected because there is a public interest in both discussion and being able to acquire information. The Court said that even if there is harm in the criticism of official conduct, citizens have First Amendment protections for such speech.245 The criticism needs “breathing space to survive.”246 The court emphasized that the theory of the Constitution is “that every citizen may speak his mind and every newspaper express its view on matters of public concern

244 *Id.* at 284-92.
245 *Id.* at 298.
246 *Id.*
and may not be barred from speaking or publishing because those in control of government think that what is said or written is unwise, unfair, false, or malicious.”

**Dombrowski v. Pfister**

The “chilling effect” was mentioned by name by the U.S. Supreme Court for the time in a decision, which found a Louisiana Law criminalizing Communist association to be unconstitutional. Although the case is related to previous decisions involving free association by organizations dissenting from government policy, it is more significant for the Court’s recognition of the “chilling effect” that government suppression has on First Amendment activities.

In *Dombrowski v. Pfister*, decided April 26, 1965, the Supreme Court, in a 5-2 vote, reversed the lower plaintiff’s conviction of the appellant for distribution of communist literature. The plaintiff, James A. Dombrowski, alleged that Louisiana’s Subversive Activities and Communist Control Law and Communist Propaganda Control Law violated his First Amendment right of free expression. The law required members of communist organizations to register with the government. He complained the laws were overbroad and used in “bad faith” to deter civil rights efforts. The United States District Court For The Eastern District Of Louisiana upheld his conviction and Dombrowski appealed the case to the Supreme Court.

The Supreme Court found that reviewing the conviction would not be “adequate vindication” for violated constitutional protections and in the interim, there might be a “substantial loss or impairment of freedoms of expression.” The court felt this would be an

---

247 Id. at 299.


249 *Dombrowski*, 380 U.S. at 492-93.

250 Id. at 485.
“irreparable injury” under the First Amendment. The Court said, “the mere possibility of
erroneous initial application of constitutional standards will usually not amount to the irreparable
injury necessary to justify a disruption of orderly state proceedings.”

The Court emphasized that regardless of prosecution, the law could create a “chilling effect
upon the exercise of First Amendment rights,” by discouraging membership and threatening
exposure of those with unpopular ideas. Addressing the danger in sweeping statutes, the
Court said

Appellants' allegations and offers of proof outline the chilling effect on free expression of
prosecutions initiated and threatened in this case.

The Court said that the Louisiana Statute, in that it was overly broad, had the potential to
create a “danger zone” where protected expressions “may be inhibited.” As long as the state
can prosecute under the statute, the threat of prosecutions pose a “real and substantial” threat to
protected expression.

Even the prospect of ultimate failure of such prosecutions by no means dispels their
chilling effect on protected expression.

In Dombrowski, the Court acknowledged the potentially harmful effect of laws
criminalizing activities protected by the First Amendment. If a law remained on the books, even

---

251 Id. at 483.
252 Id. at 484.
253 Id. at 488, 494.
254 Id. at 487 (citing N.A.A.C.P. v. Button, 371 U. S. 433 (1963), where the Court ruled on a case involving attorney
malpractice and solicitation of business. In the case, the Court addressed the potential effect of successful
prosecution “The chilling effect upon the exercise of First Amendment rights may derive from the fact of the
prosecution, unaffected by the prospects of its success or failure.”)
255 Id. at 494.
256 Id.
257 Id.
when charges filed under the law failed, the law still had the potential to alter citizens’
constitutionally protected activities by creating fear of official government retribution. The
“danger zone” referenced by the Court is antonymous with the idea of “breathing space.”
Citizens, denied a breathing zone to engage in First Amendment expression and association free
from government action, could potentially “chill” their activities in order to escape prosecution.
Any chilling of citizen expression could effect the competition of ideas in the marketplace.

**Lamont v. Postmaster General**

Another case of government suppression of subversive views involves the distribution of
communist literature through the United States Postal System. The Lamont case focused more
clearly on free association, as it was decided upon a “right to receive.” In *Lamont v. Postmaster
General*, decided May 24, 1965, the U.S. Supreme Court, in an 8-0 vote, found the Postal
Service and Federal Employees Salary Act of 1962 to be an unconstitutional abridgement of
citizen’s First Amendment rights.\(^{258}\) The 1962 Act required the Postmaster General to detain
unsealed mail from foreign addressees of “communist political propaganda” and deliver the held
mail only when the addressee requested it through signing a notification card.\(^{259}\) Under the Act,
the postal service maintained screening points where all unsealed mail from designated countries
was routed.\(^{260}\) For a three-year period, the notification card contained a check box where the
addressee could indicate a desire to receive “communist political propaganda” in the future.\(^{261}\)
The postmaster maintained a list of addressees requesting this kind of correspondence.\(^{262}\)

---

\(^{258}\) Lamont v. Postmaster Gen., 381 U.S. 301 (1965); Postal Service & Federal Employees Salary Act of 1962, 76
Stat. 840 §305 (a) (1962).

\(^{259}\) Lamont, 381 U.S. at 302-04.

\(^{260}\) Id.

\(^{261}\) Id.

\(^{262}\) Id.
Corliss Lamont sued the Post Office, arguing that the requirement to be listed was a violation of his First Amendment rights of free association.

The majority opinion, written by Justice Douglas, found that the addressee’s First Amendment rights were limited by requiring him to return the card in order to receive mail.\textsuperscript{263} In the opinion, the Court likened the maintenance of the list to a licensing act that controlled the flow of ideas to the public.\textsuperscript{264} The list was found to have a deterring effect to correspondence by those with “sensitive positions.”\textsuperscript{265} The Court said the Postal Service Act “is at war with the uninhibited, robust, and wide-open debate and discussion that are contemplated by the First Amendment.”\textsuperscript{266}

In a concurring opinion, Justice William Brennan wrote that although there is no specific constitutional guarantee for access to publications, the Bill of Rights protects fundamental personal rights “necessary to make the express guarantees fully meaningful.”\textsuperscript{267} Brennan argued that a “right to receive” is fundamental and necessary so that addressees can receive ideas and be free to consider them.\textsuperscript{268} Brennan argued that the alternative “would be a barren marketplace of ideas” with only sellers and no buyers.\textsuperscript{269} Brennan cites the reasoning in 1926 Supreme Court case, \textit{Boyd v. United States}, involving the a defendant charged with failing to pay import duties on a shipment of plate glass.\textsuperscript{270} At the district court trial, the defendant successfully argued that

\begin{flushleft}
\textsuperscript{263} \textit{Id.} at 305-07.
\textsuperscript{264} \textit{Id.} at 306.
\textsuperscript{265} \textit{Id.} at 307.
\textsuperscript{266} \textit{Id.} (citing N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964)).
\textsuperscript{267} \textit{Id.} at 308.
\textsuperscript{268} \textit{Id.}
\textsuperscript{269} \textit{Id.}
\textsuperscript{270} \textit{Id.} at 309.
\end{flushleft}
producing the invoice would result in self-incrimination, a violation of his constitutional rights under the Fifth Amendment. The Supreme Court upheld the decision, reasoning:

It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. This can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed. A close and literal construction deprives them of half their efficacy, and leads to gradual depreciation of the right, as if it consisted more in sound than in substance. It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.271

The Lamont case was the first time the Supreme Court declared a federal law unconstitutional on First Amendment grounds. It was also the first time the Court used the phrase “marketplace of ideas,” although the term “market” had been used before by Holmes and Brandeis in the Abrams dissent, and later in Brandeis’ dissent to the Gitlow case. This recognition, by a Court majority, is significant in establishing a judicial theory around the “chilling effect” of government actions on free expression. In the Lamont decision, the Court—although not by name—began to establish a need for “breathing space” to protect free expression in the marketplace of ideas.

Ashton v. Kentucky

In the late 1960’s the Court began to strengthen protections for free expression under the First Amendment. Although they did not use the term “breathing space” in these opinions, the holdings implied a stricter standard for laws that criminalized constitutionally protected activities. In Ashton v. Kentucky, decided May 16, 1966, the U.S. Supreme Court held that a conviction, under a broad construction of law that make it unconstitutional, cannot be sustained.

---

The Court granted certiorari and reversed the lower court decision.

Ashton was convicted for violating the Kentucky common law crime of criminal libel—defined as “any writing calculated to create disturbances of the peace, corrupt the public morals, or lead to any act which, when done, is indictable.” His crime was the publication of a pamphlet. The pamphlet accused Hazard Police Chief Sam L. Luttrell of having a side job, even though it was illegal for “peace officer to take private jobs.” It said Sheriff Charles E. Combs hired deputies because they wanted to carry guns. The pamphlet also said Combs intentionally blinded a boy with teargas and beat him up while he was handcuffed, in a locked jail cell. The pamphlet suggested that Comb “probably bought off the jury,” in the related trial. Finally, the pamphlet said that the co-owner of the Hazard Herald, Mrs. W.P. Nolan, was accused of withholding national aid shipments to miners.

The petitioner was charged with malice and falsity, both requirements of the offence. He was sentenced to prison and fined for the publication of a pamphlet that made claims against police officials involved in a Kentucky labor dispute. The Kentucky Court of Appeals affirmed the conviction, but adopted a different definition of criminal libel removing the requirement that breach of the peace be the constitutional basis for imposing criminal liability.

---

273 Id. at 197.
274 Id. at 196.
275 Id.
276 Id. at 197.
277 Id.
278 Id. at 196.
279 Id. at 197.
The Supreme Court found that the laws under which the petitioner was convicted were vague. “Laws which touch on First Amendment rights must be carefully and narrowly drawn.” The majority opinion emphasized that civil and political institutions depend on free discussion. The right to speak freely and promote diverse ideas is what sets the United States apart from totalitarian regimes.

Stanley v. Georgia

In Stanley v. Georgia, decided April 7, 1969, the U.S. Supreme Court, in a 9-0 vote, held that the First and Fourteenth Amendments prohibited a Georgia statute criminalizing the private possession of obscene materials. In Stanley, law enforcement officers searched the plaintiff’s home for evidence of illegal materials involving bookmaking. While executing the search warrant, they found reels of film containing obscene images. The film was seized and Stanley was convicted under Georgia law for possession of obscene materials.

The conviction was upheld by the Supreme Court of Georgia and appealed to the U.S. Supreme Court. In the majority opinion for the U.S. Supreme Court, Justice Thurgood Marshall recognized the right to receive information, in the privacy of one’s own home, as a fundamental right protected by the constitution. The Court held that a state could regulate production or distribution of obscene material, but not private possession. This decision, like

---

280 Id. at 200.
281 Id. at 198-200.
283 Id. at 558.
284 Id.
285 Id.
286 Id. at 565.
287 Id. at 567-68.
*Lamont*, upheld the right of the plaintiff to receive information from other citizens as an important constitutional protection.

**Brandenburg v. Ohio**

The *Dennis* case was overruled in 1969 by *Brandenburg v. Ohio* allowing the court to reinterpret the “clear and present danger” test to more stringently require “imminent action,” rather than the previous standard of “clear and present danger” established in *Schenck*. In *Clarence Brandenburg v. State of Ohio*, decided June 9, 1969, the U.S. Supreme Court in a unanimous decision, held that Ohio’s criminal syndicalism statute violated the First Amendment, applied through the Fourteenth Amendment because it broadly prohibited the mere advocacy of violence, not the constitutionally unprotected incitement to imminent lawless action.\(^\text{288}\)

Imminent lawless action required “intent”, “imminence” and “likelihood.”

Ohio Ku Klux Klan leader Clarence Brandenburg invited a Cincinnati Television station to cover a KKK rally, portions of which were taped and showed group members making speeches, including a speech where a member said "our President, our Congress, our Supreme Court, continues to suppress the white, Caucasian race."\(^\text{289}\) The member subsequently announced plans for a July 4\(^\text{th}\) march on Washington.\(^\text{290}\) Brandenburg was charged and convicted for advocating “the duty, necessity, or propriety of crime, sabotage, violence, or unlawful methods of terrorism as a means of accomplishing industrial or political reform" and "voluntarily assembl[ing] with any society, group or assemblage of persons formed to teach or advocate the doctrines of criminal syndicalism." Brandenburg was convicted under the statute. He argued that the statute

---


\(^{289}\) *Id.* at 444-45.

\(^{290}\) *Id.* at 445-46.
violated his First and Fourteenth Amendment rights to freedom of speech. An Ohio Appellate Court upheld his conviction.

The Supreme Court reversed Brandenburg’s conviction since the statute punished “mere advocacy” of action. The Court added, “Freedoms of speech and press do not permit a State to forbid advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.”

In Brandenburg, the court writes that its decisions have fashioned the principle that the constitutional guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.

Justice Douglas, in his concurring opinion, agreed with the Court, but said he did not believe the “clear and present danger test” had a place in the First Amendment regime.

Action is often a method of expression, and within the protection of the First Amendment. Suppose one tears up his own copy of the Constitution in eloquent protest to a decision of this Court. May he be indicted? Suppose one rips his own Bible to shreds to celebrate his departure from one "faith" and his embrace of atheism. May he be indicted?

He reiterated the “line between what is permissible and not subject to control and what may be made impermissible and subject to regulation is the line between ideas and overt acts.”

Justice Black in his concurrence agreed with Justice Douglas’ concurring opinion that the "clear and present danger" doctrine should have no place in the interpretation of the First Amendment.

---

291 Id. at 444.
292 Id. at 447. One action found not to incite action against the government is the act of burning a United States flag. In 1989, in Texas v. Johnson, the Supreme Court reversed the conviction of Gregory Johnson for burning a flag, determining that an idea cannot be punished simply because “society finds the idea offensive or disagreeable.” This decision is seen as a protection of free expression. Texas v. Johnson, 491 U.S. 397 (1989).
293 Brandenburg, 395 U.S. at 454.
294 Id. at 454-55.
295 Id. at 456.
Amendment.  He joined with the Court’s opinion citing Dennis, but pointed out that the per curium opinion did not indicate any agreement on the Court's part with the "clear and present danger" doctrine on which Dennis purported to rely.

Brandenburg was the Court’s last major case involving government suppression of speech that might incite others to lawless action. The Brandenburg test validated Justices Holmes and Brandeis’ dissents in the opinions immediately following Schenck.

Gertz v. Welch

The Court, following Brandenburg, continued to provide stricter standards laws that criminalized activities that enjoyed constitutional protections, such as public discussion. In Elmer Gertz v. Robert Welch, Incorporated, decided June 25, 1974, the U.S. Supreme Court reversed the Seventh Circuit Court’s opinion and held that the First Amendment permitted statutes that formulated their own standards of libel for defamatory statements made upon private figures, as long as liability is not imposed without fault. Justice Lewis Powell wrote the majority opinion, joined by Justices Potter Stewart, Thurgood Marshall, Harry Blackmun and William Rehnquist. Justice Harry Blackmun concurred. Chief Justice Warren E. Burger, and Justices William Brennan, William Douglas and Byron White dissented in four individual opinions.

Chicago policeman, Nuccio, was convicted of second-degree murder. The victim’s family retained the petitioner, Elmer Gertz, “a reputable attorney,” to represent them in civil litigation against Nuccio. The American Opinion, a publication of the John Birch Society,

---

296 Id. at 450.
298 Id. at 325-26.
299 Id.
“alleged” the murder trial was part of a “Communist conspiracy to discredit the local police.”\textsuperscript{300} The article said Gertz arranged Nuccio’s “frame-up,” and called Gertz a “communist-fronter.”\textsuperscript{301}

Gertz filed a libel suit against the publisher of the magazine, Robert Welch, and the jury of the United States District Court for the Northern District of Illinois found for Gertz.\textsuperscript{302} Gertz claimed that the “falsehoods published by the respondent injured his reputation as a lawyer and a citizen.”\textsuperscript{303} After the jury returned its verdict, the District Court decided to apply the \textit{New York Times v. Sullivan} standard barring “media liability for defamation of a public official absent proof that the defamatory statements were published with knowledge of their falsity or in reckless disregard of the truth, should apply to this suit.” Gertz appealed the decision contesting the applicability of the \textit{New York Times} standard, since he was not a public figure.\textsuperscript{304} The Court of Appeals would affirm this decision, which found that Gertz failed to prove “knowledge of falsity or “reckless disregard for the truth.”\textsuperscript{305}

The Supreme Court reversed and remanded the lower court decision deciding the case on the issue of “whether a newspaper or broadcaster that publishes defamatory falsehoods about an individual who is neither a public official nor a public figure may claim a constitutional privilege against liability for the injury inflicted by those statements.”\textsuperscript{306} This led to a judicial analysis of true and false ideas, which would shape future decisions involving government restriction of free

\begin{footnotesize}
\begin{enumerate}
\item \textit{Id.}
\item \textit{Id.}
\item \textit{Id.} at 327.
\item \textit{Id.} at 330.
\item \textit{Id.} at 332.
\end{enumerate}
\end{footnotesize}
speech. The Court said there is “no such thing as a false idea” under the First Amendment. Although there may be no constitutional value in false statements of fact, they provide competition for other ideas within the marketplace. When the state punishes false opinions, it runs the risk of “inducing a cautious and restrictive exercise of the constitutionally guaranteed freedoms of speech and press.”

Relying upon the *New York Times* decision, the Court said that there must be an “allowance of the defense of truth,” allows the propagation of speech “that matters”, however, the Court did not apply the *New York Times* standard.

In his dissenting opinion, Justice Brennan agree with the Court’s holding that the petitioner was not a public official or figure, but he argued that the decision offered no “breathing space” for free and robust debate. Brennan emphasized that “even a limitation of recovery to actual injury,” would do little to give First Amendment expression the “elbowroom” it needs to flourish. Finally, even a limitation of recovery to “actual injury” - however much it reduces the size or frequency of recoveries - will not provide the necessary elbowroom for First Amendment expression. Justice White also dissented, applying *New York Times* standard for seditious libel as “beyond the police power of the state.”

---

307 *Id.* at 339.
308 *Id.*
309 *Id.* at 340.
310 *Id.* at 341.
311 *Id.* at 361.
312 *Id.* at 367.
313 *Id.* at 387.
Breathing Space

The term “breathing space” was used by the Court in the *Times* decision, there are also references to this concept in other Court opinions that are not as closely related to this review of the chilling effect of government action. Still, these cases will be reviewed briefly to show a growing use of the term by the Court. Collectively, the cases begin to clarify the Court’s use of the term and how it should be applied in First Amendment protections.

In the 1986 case of *Philadelphia Newspapers v. Hepps*, the U.S. Supreme Court expanded the idea of breathing space for “true speech” on matters of public concern.314 In the case, a Pennsylvania libel statute was found unconstitutional on First Amendment grounds. The Court reasoned that First Amendment expressions require "'breathing space.'"315 The kind of speech in question concerned the nature of the political process. The Court found this kind of speech “clearly” mattered and was at the core of First Amendment protections—even if the speech was false.

In the 1988 case of *Hustler Magazine v. Jerry Falwell*, the U.S. Supreme Court found that a parody of a public figure had First Amendment protection.316 The Court recognized that even falsehoods have value in political debate and restricting speech of this nature would have a chilling effect on speech that has Constitutional value. The Court cited *Philadelphia Newspapers* to reiterate that protection for free expression under the First Amendment requires “breathing space.”


315 *Id.* at 799.

Virginia v. Black

In Commonwealth of Virginia, Petitioner, v. Barry Elton Black, Richard J. Elliott, and Jonathan O’Mara, decide April 7, 2003, the U.S. Supreme Court upheld the constitutionality of part of a Virginia statute banning cross burning, but struck down the part of the statute requiring the defendant to bear the burden of proof in demonstrating that the act of burning a cross was not intent as intimidation. 317

Justice Sandra Day O’Connor wrote parts I-III of the majority opinion and parts IV and V of the concurrence. Her majority opinion was joined by Chief Justice William Rehnquist, and Justices John Paul Stevens, Antonin Scalia and Stephen Breyer. O’Connor’s concurrence was joined by Rehnquist, Stevens and Breyer. Justice John Paul Stevens also wrote a concurrence, as did Justice Antonin Scalia who also dissented in part and was joined by Justice Clarence Thomas for parts I and II of his dissent. Justice David Souter, joined by Justices Anthony Kennedy and Ruth Bader Ginsburg concurred and dissented in part. Clarence Thomas also authored a dissent.

Barry Elton Black was convicted of violating a Virginia Statute banning cross burning. The Court struck down the statute because it used the act of cross burning as prima facie evidence of intent to intimidate. The First Amendment’s protection for speech are not absolute and free speech and expression “may” be regulated in certain categories. 318 The state could ban cross burning when there was the intent to intimidate. 319

Although the Virginia decision struck down the cross-burning statute in part, it did create some vulnerability for First Amendment activities that had the tendency to “intimidate.” This reliance on the “intent” of the action was reminiscent of the Court’s opinions during the Schenck


318 Id. at 344.

319 Id.
era when the “clear and present danger” test was formulated. Given the recency of this case, its influence on judicial interpretations of First Amendment protections cannot be well established.

The First Amendment cases reviewed in this section have established a clear test of “clear and present danger” for evaluating the government’s criminalization of constitutionally protected activities. Although some of these cases involve prosecution for libel, most cases involved prosecution of citizens expressing views that were different from democratic ideals, or the military goals of the government during war time. In reviewing these cases, the “chilling effect” of government actions on the marketplace of ideas emerged as a line of reasoning used by the Court to evaluate the use of the “clear and present danger” test. The phrases “chilling effect”, “marketplace of ideas” and “breathing space” were not only used by the Court, but the underlying principles involving the concepts were applied first in dissents and later in majority holdings as valuable ideas for evaluating First Amendment protections.

**Fourth Amendment Decisions**

The Fourth Amendment protects against unreasonable search and seizure, search without warrant, and search without probable cause. The amendment—which textually protects people, homes, papers and effects—was in large part of a reaction to writs of assistance imposed on the colonist during the time of British rule.\(^320\) The Fourth Amendment states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.\(^321\)

Although the relevance of the “chilling effect”, “marketplace of ideas”, and “breathing space,” is clear in the First Amendment cases discussed in the previous section, the cases

---

\(^320\) A “writ of assistance” is a general search warrant. See definitions, *supra* Chapter 1.

\(^321\) [U.S. CONST. amend. IV.](#)
reviewed up to this point did not involve electronic surveillance. Citizens now use electronic communication—specifically phone communication—to engage in political discourse and other First Amendment activities. This section will review the Court’s seminal decisions involving the application of the Fourth Amendment to electronic surveillance by the government. Notably, the first Fourth Amendment cases involving electronic surveillance decided by the Court do not extend the Fourth Amendment’s protection for unwarranted search and seizure. As the Court began to change its early reasoning and extend Fourth Amendment protections for electronic surveillance, the judicial reasoning relied on in decisions begins to highlight the necessity of extending the marketplace model to electronic communications. The cases in this section will be reviewed chronologically, following the Court’s gradual adoption of the Fourth Amendment’s protections for electronic surveillance case. The review will also highlight the emergence of the marketplace model—and the related ideas of “chilling effect” and “breathing space”—in the Court’s opinions involving electronic surveillance.

The cases that will be discussed reveal a shift in the Court’s treatment of phone communication. At first, in *Olmstead*, the Court was hesitant to extend the same protections to electronic communication that were provided to letters sent through the United States Postal Service. Essentially, phone communication was seen as a sort of broadcast made for anyone with the ability to intercept the transmission. In subsequent cases, the Court changed its reasoning, and recognized the privacy rights of parties involved in electronic transmissions. This reasoning would be based in part on the necessity of citizens to use phone communications as a tool for public discussion in the marketplace.

**Olmstead v. United States**

In *Olmstead et al. v. United States*, decided April 9, 1928, the U.S. Supreme Court, in a 5-4 decision, affirmed the decision of the Ninth Circuit of the U.S. Court of Appeals, finding that
the tapping of private conversations—over telephone wires leading from the defendants’
residence to office where conspiracy was allegedly planned—was not an unlawful search and
seizure under the Fourth Amendment.\(^{322}\)

The plaintiffs, including Roy Olmstead, were convicted of a conspiracy to violate the
National Prohibition Act in the District Court for the Western District of Washington. They
were charged with unlawfully “possessing, transporting, and selling alcohol.” Olmstead was the
general manager of a Seattle bootlegging facility. The conspiracy was discovered in part by
federal officers who tapped the phones of the conspirators.\(^{323}\) “Small wires” were inserted along
the telephone wires in the basement of the building and at the house lines in the streets near the
house, without trespassing on the property of the defendants.\(^{324}\)

The majority opinion was written by Chief Justice William Taft, joined by Justices James
McReynolds, Edward Sanford, George Sutherland, and Willis Van Devanter.\(^{325}\) The Court relied
upon several cases to decide the case. \textit{Boyd v. United States}, decided February 1, 1886, was a
case involving the seizure and forfeiture against 35 cases of plate glass by the District Attorney
after the owner/importer of the glass used fraudulent or false invoices to defraud revenue.\(^{326}\) The
“Congressional Act of 1874,” compelling the production of the invoice for inspection, was found
to be “repugnant” to the Fourth and Fifth Amendments because the refusal to produce the
documents was equated by the Court with an admission of guilt.\(^{327}\)


\(^{323}\) Olmstead v. United States, 277 U.S. 438 (1928).

\(^{324}\) \textit{Id.} at 457.

\(^{325}\) Justices Louis Brandeis, Oliver Holmes, Harlan Stone and Pierce Butler dissented in four different opinions.

\(^{326}\) Olmstead, 277 U.S. at 458 (citing Boyd v. United States, 116 U. S. 616 (1886)).

Justice Joseph Bradley—relying on the Court’s decision in *Boyd v. United States*—said the Fourth Amendment issue in the *Olmstead* case as the government’s “compelling” production of the invoices if the defendant did not produce them.\(^{328}\) Although this is not “actual search and seizure, it does force the defendant to produce self-incriminating evidence.”\(^{329}\) The Court in the *Boyd* case found that “compulsory production of a man’s private papers to establish a criminal charge against him” was a Fourth Amendment issue of search and seizure.\(^{330}\)

The Court in *Olmstead* also relied upon the reasoning in *Weeks v. United States*, decided February 24, 1914, to establish that a warrant was needed to engage in search and seizure under the Fourth Amendment.\(^{331}\) In the *Weeks* case, police arrested the defendant without a warrant and then searched the defendant’s room after obtaining a key from the neighbor.\(^{332}\) Although they did not possess a search warrant, they seized “various papers and articles.”\(^{333}\) The defendant requested his property be returned and the lower court ordered the return of items not related to the case. The Court, drawing a parallel between personal items in the home and sealed letters in the mail, held that an official of the United States had acted “under color” of his office and violated the defendants’ constitutional rights in seizing the items without a warrant.\(^{334}\) This was the first use of the exclusionary rule, barring the admission of illegally obtained evidence in court.

---

\(^{328}\) *Boyd*, 116 U. S. at 621.

\(^{329}\) *Id.*

\(^{330}\) *Olmstead*, 277 U.S. at 459.


\(^{332}\) *Id.*

\(^{333}\) *Id.*

\(^{334}\) *Olmstead*, 277 U.S. at 460.
Finally, the Court in *Olmstead* looked at Fourth Amendment warrant requirements in the case of *Gouled v. United States*, decided February 28, 1921, where the defendant was charged with conspiracy to defraud the United States after a document was taken from his office under the orders of the Intelligence Department of the Army.\(^{335}\) The paper, which incriminated him, was taken without a warrant, given to the United States attorney and introduced as evidence in the conspiracy.\(^{336}\) Admission of the paper in the lower court was considered a violation of the Fourth Amendment because the defendant had no knowledge of its admission to court and could not request its return before it was introduced and considered by the court.\(^{337}\)

The Supreme Court used the *Boyd*, *Weeks* and *Gouled* cases to rule out a Fifth Amendment claim of compelled speech and instead focus on the Fourth Amendment issue of warrants.\(^{338}\) The Court relied on the historical purpose of the Fourth Amendment to “prevent the use of governmental force to search a man’s house, his person, his papers, and his effects and to prevent their seizure against his will.”\(^{339}\) In the *Boyd* and *Weeks* cases, the issue was the government using its power to compel the production of documents.\(^{340}\) In *Gouled*, the prohibition on search and seizure was taken to the “extreme limit,” but the *Olmstead* Court said this did not expand the authority the government’s authority because in *Olmstead* there was not actual entrance of private quarters, nor was anything “tangible” seized.\(^{341}\) The Court said in *Olmstead* that it would

\(^{335}\) Gouled v. United States, 255 U. S. 298 (1921).

\(^{336}\) Id.

\(^{337}\) *Olmstead*, 277 U.S. at 462.

\(^{338}\) Id.

\(^{339}\) Id. at 463.

\(^{340}\) Id.

\(^{341}\) Id.
be impossible to obtain a warrant specifying the place person or things to be searched or seized.\textsuperscript{342} The Supreme Court said that the Fourth Amendment did protect sealed letters in the care of the Post Office from government seizure, but conversations conducted over phone lines were different in several ways. First, the postal service is monopolized by the government and “unlawful rifling” by government agents would be “search and seizure” of a senders’ “effects, which are only transmittable by use of the government’s mail system, which has guaranteed protection.”\textsuperscript{343} The telegraph and telephone systems do not have this protection because they do not involve personal “effects,” but rather communications “reaching to the whole world from the defendant’s home or office.” Second, intercepting phone communications involves only “hearing,” not seizure. Third, the Court suggested that phone lines are open spaces like highways that stretch between houses, and therefore are not guaranteed protection from search and seizure.\textsuperscript{344}

Despite the fact that the \textit{Gouled} Court urged liberal interpretation of the “purpose of the framers of the Constitution in the interest of liberty,” it did not extend search and seizure beyond “persons, papers, and effects” to “hearing and sight.”\textsuperscript{345} This is because although cases of

\begin{footnotesize}
\begin{enumerate}
\item \textit{Olmstead}, 277 U.S. at 464.\textsuperscript{342}
\item \textit{Id.}\textsuperscript{343}
\item \textit{Id.} at 464-65.\textsuperscript{344}
\item \textit{Id.} at 465.\textsuperscript{345}
\end{enumerate}
\end{footnotesize}

The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The Fourth Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants…By the invention of the telephone 50 years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place…The language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.
government intrusion on phone lines might involve trespass, they did not trigger Fourth Amendment protection because there was no potential for anything tangible to be seized as evidence. 346 The Court suggested that only Congress could change the laws protecting the secrecy of telephone communications. 347 If someone installs a telephone in his or her home, he has the intention of projecting his voice across the wires running from the house. For this reason, the Fourth Amendment does not apply because the person has no tangible effect to protect and the interception does not take place in their home. 348

It is important to note that although *Olmstead* is a landmark decision in which the court denied Fourth Amendment protection for phone communications, four justices dissented from the majority opinion, offering multiple interpretations of the constitution over the holding’s literalist interpretation.

Justice Louis Brandeis, in his dissent, emphasized that the “illegal wiretapping” was an “unreasonable search and seizure” given that it lasted for many months and involved the tapping of eight telephones. 349 He wrote that the telephone is an instrument that the American Constitutional framers “could not have dreamed of,” 350 and legislation should be adaptable to

---

346 *Id.* See Hester v. United States, 265 U. S. 57 (1924) (holding that “the testimony of two officers of the law who trespassed on the defendant’s land, concealed themselves 100 yards away from his house, and saw him come out and hand a bottle of whisky to another, was not inadmissible. While there was a trespass, there was no search of person, house, papers, or effects). See also United States v. Lee, 274 U. S. 559 (1927).

347 *Olmstead*, 277 U.S. at 465.

348 “What has been said disposes of the only question that comes within the terms of our order granting certiorari in these cases. But some of our number, departing from that order, have concluded that there is merit in the twofold objection, overruled in both courts below, that evidence obtained through intercepting of telephone messages by a government agents was inadmissible, because the mode of obtaining it was unethical and a misdemeanor under the law of Washington. To avoid any misapprehension of our views of that objection we shall deal with it in both of its phases.” *Id.* at 466.

349 *Id.* at 471 (Brandeis, J., dissenting).

350 “We must never forget,” said Mr. Chief Justice Marshall in [McCullough v. Maryland] ‘that it is a Constitution we are expounding.’ Since then this court has repeatedly sustained the exercise of power by Congress, under various
modern circumstances, not “confined to the form that evil had theretofore taken” in past experiences. When the framers wrote the constitution “force and violence” were the only method the government could use to compel self-incrimination.

Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.

Brandeis, in his dissent, predicted that the government might one day have even more “scientific” ways of invading individual security, that perhaps may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

Relying on *Boyd v. United States*, Brandeis said that the government is not only supposed to respect concrete forms of property such as doors, but also the “indefeasible right of personal security, personal liberty and private property.” Citing the reasoning in *Interstate Commerce Commission v. Brimson* (1894), a case that relied on *Boyd*, Brandeis invoked the words of the Court:

> Of all the rights of the citizen, few are of greater importance or more essential to his peace and happiness than the right of personal security, and that involves, not merely protection of his person from assault, but exemption of his private affairs, books, and papers from the clauses of that instrument, over objects of which the fathers could not have dreamed.” *Id.* at 472 (quoting McCulloch v. Maryland, 17 U.S. 316 (4 Wheat.) (1819).

---

351 *Id.* at 472.
352 *Id.* at 473.
353 *Id.*
354 *Id.* at 474.
355 116 U. S. 616 (1886).
356 *Olmstead*, 277 U.S. at 475.
inspection and scrutiny of others. Without the enjoyment of this right, all other rights would lose half their value.\footnote{Id. (citing Interstate Commerce Commission v. Brimson, 154 U. S. 447, 479 (1894) (holding that the twelfth section of an 1887 act to regulate commerce—authorizing the Commerce Commission to invoke the aid of any U.S. court in requiring the “attendance and testimony of witness, and the production of documents, books, and papers”—was constitutional because the matter extended beyond the Court’s judicial power)).}

In regards to the specific comparisons between mailed letters and phone communications, Brandeis relied on the words of Ninth Circuit Court of Appeals District Judge Frank Rudkin from the \textit{Ex parte Jackson} case to write that there is no essential difference between the two.\footnote{Id. (citing \textit{Ex parte Jackson}, 96 U.S. 727 (1878) (holding that publications relating to illegal lotteries could be excluded from mailing by the U.S. postal service)).} Brandeis even went so far as to suggest that phone tapping involved the invasion of multiple parties’ privacy because the phone lines of everyone that communicated with the suspect were tapped when they contacted or were contacted by him.\footnote{Id. at 476.} Brandeis said, “writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping.”\footnote{Id. at 476.}

Brandeis emphasized that the Constitutional framers recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the [sic] most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.\footnote{Id. at 478.}

Brandeis reasoned that it should not matter if the evidence was acquired by a physical search and seizure or it aided law enforcement. He said that liberty should be protected,
especially when “government’s purposes are beneficent,” because “the greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.”362

Brandeis referenced a brief filed by the telephone companies in the case,

Criminals will not escape detection and conviction merely because evidence obtained by tapping wires of a public telephone system is inadmissible. if it should be so held; but, in any event, it is better that a few criminals escape than that the privacies of life of all the people be exposed to the agents of the government, who will act at their own discretion, the honest and the dishonest, unauthorized and unrestrained by the courts. Legislation making wire tapping a crime will not suffice if the courts nevertheless hold the evidence to be lawful.363

Brandeis said that the Radio Act of 1927, as well as numerous state laws, banned wiretapping by private parties or the government.

Decency, security, and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen. In a government of laws, existence of the government will be imperiled if it fails to observe the law scrupulously. Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means-to declare that the government may commit crimes in order to secure the conviction of a private criminal-would bring terrible retribution.364

Justice Oliver Holmes dissented separately, but agreed with Brandeis on this last point regarding government conduct.365 Justice Pierce Butler also dissented, agreeing with Brandeis and Holmes on the issue of the government following the law, but added:

Telephones are used generally for transmission of messages concerning official, social, business and personal affairs including communications that are private and privileged-those between physician and patient, lawyer and client, parent and child, husband and wife. The contracts between telephone companies and users contemplate the private use of the facilities employed in the service. The communications belong to the parties between

362 Id. at 479.
363 Id.
364 Id. at 484.
365 Id.
whom they pass. During their transmission the exclusive use of the wire belongs to the persons served by it. Wire tapping involves interference with the wire while being used. Tapping the wires and listening in by the officers literally constituted a search for evidence. As the communications passed, they were heard and taken down. 366

_**Olmstead**_ was followed by a series of progeny cases would shape surveillance law in the coming decades. The first case involving “bugging,” or surveillance by an electronic device, to reach the Supreme Court was _Goldman v. United States_, decided April 22, 1942. 367 The case involved a device called a detectaphone that was placed against a wall to overhear conversations in an adjoining the room. In this case, the Court found that “bugging” did not violate Fourth Amendment rights since there was no physical trespass during the interception. In _On Lee v. United States_, decided February 23, 1982, the Court found that “no trespass was committed” when a federal agent bugged the target’s laundry. 368 In _Silverman v. United States_, decided March 6, 1961, the Court found that a microphone inserted under a baseboard to electronically eavesdrop on a target’s conversations did constitute an “actual intrusion into a constitutionally protected area.” 369

In _Olmstead_, the Court upheld the constitutionality of warrantless wiretapping by federal agents. The case was decided in the same era as the _Gitlow_ and _Whitney_ cases. In _Gitlow_ and later, _Whitney_, the Court had upheld the constitutionally of a statutes criminalizing the advocacy of violent overthrow of the government. In all three cases, the Court yielded to the government in its judgment of criminalizing what might be understood as constitutionally protected activities. In _Gitlow_ and _Whitney_, free speech was limited when it posed a danger to the nation. In

---

366 _Id._ at 487 (Butler, J., dissenting). Justice Stone also dissented.
Olmstead, private communication was not afforded Fourth Amendment protection from warrantless search and seizure when parties to the communication were engaged in conspiracy against federal statutes.

In Olmstead, the Court began to interpret how laws would be applied to the emerging telecommunications technology increasingly available to citizens. The case was decided just one year after the passage of the Radio Act of 1927. Notable is the Court’s metaphor of phone lines as “highways” exempt from traditional protection for search and seizure.\(^{370}\) It likened telephone communications to open broadcasts. The Court reasoned that there was nothing “tangible to be seized” in phone communications.\(^{371}\) The Court’s suggestion that Congress update communications law is also important because in 1934, Congress would pass the Communications Act, legalizing carrier cooperation with government efforts during national emergencies.\(^{372}\)

Lopez v. United States

In Lopez v. United States, decided May 27, 1963, the U.S. Supreme Court, in a 6-3 vote, affirmed the Federal District Court of Massachusetts’ decision that the Internal Revenue Service was not guilty of unlawfully invading the German Lopez’s office because the defendant gave

---

\(^{370}\) "The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants…By the invention of the telephone 50 years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place…The language of the amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.” Olmstead v. United States, 277 U.S. 438, 464-65 (1928).

\(^{371}\) Id. See Hester v. United States, 265 U. S. 57 (1924). In Hester, the Court held that the testimony of two officers of the law who trespassed on the defendant's land, concealed themselves 100 yards away from his house, and saw him come out and hand a bottle of whisky to another, was not inadmissible. While there was a trespass, there was no search of person, house, papers, or effects. See also United States v. Lee, 274 U. S. 559 (1927).

\(^{372}\) Commc’ns Act, 47 U.S.C. § 151 (1934).
consent for entry and the agent’s willingness to accept a bribe was “not real.” The defendant was indicted and convicted on four counts of attempted bribery of Internal Revenue Agent Roger Davis based in part on a wire recording of a conversation in which the bribe took place. Justice Harlan wrote the majority opinion, joined by Justices Warren, Black, Clark, Stewart and White. Justices Douglas and Brennan dissented. The decision hinged on the fact—under Massachusetts law—that Davis was party to the recording, not a third party, and simply used the wire-recorded conversation to verify his testimony. The surveillance device was not planted by “unlawful physical invasion of a constitutionally,”—‘eavesdropping’— it was simply worn by the agent. The Court concluded that the petitioner accepted the chance of “faultless memory or mechanical recording” when he invited the agent inside for a conversation. The Court reasoned that the risk that taken by the Lopez in offering a bribe to the federal agent included the risk that the offer would be accurately reproduced in court, “whether by faultless memory or mechanical recording.”

Chief Justice Earl Warren concurred with the majority opinion, but emphasized that the current decision did not reaffirm the On Lee decision, which upheld the use of a wired information to collect evidence. With Justice William Brennan joining, Warren said that 1) the On Lee case was wrongly decided; 2) “fantastic advances in the field of electronic

---

373 Lopez v. United States, 373 U.S. 427, 438-43 (1963). In Lopez, the defendant was charged with bribing an internal revenue service agent. The Court affirmed the lower court decision that electronic eavesdropping devices were constitutional if not planted through “unlawful physical invasion of a constitutionally protected area.”

374 Id. at 428.

375 “The Court has, in the past, sustained instances of ‘electronic eavesdropping’ against constitutional challenge, when devices have been used to enable government agents to overhear conversations which would have been beyond the reach of the human ear.” Id. at 438.

376 Id. at 439.

377 Id. See also Lee v. United States, 343 U.S. 747 (1952).

378 Lopez, 373 U.S. at 441.
communication constitute a great danger to the privacy of the individual; 3) indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments; and 4) and these considerations impose a heavier responsibility on this Court in its supervision of the fairness of procedures in the federal court system. 379

Justice Brennan, joined by Justices William Douglas and Arthur Goldberg dissented, writing that the purpose of the Fourth Amendment is not just to protect secrecy. Brennan added that Lopez did not surrender his “right of privacy when he communicated his ‘secret thoughts.’”380 Relying on Silverman v. United States, Justice Brennan said “If a person commits his secret thoughts to paper, that is no license for the police to seize the paper; if a person communicates his secret thoughts verbally to another, that is no license for the police to record the words.”381 Stopping short of saying that “all communications are privileged,” Brennan added that “the right of privacy would mean little if it were limited to a person’s solitary thoughts, and so fostered secretiveness. It must embrace a concept of the liberty of one's communications, and historically it has.”382 Brennan said that the only way to guard against contemporary eavesdropping is to “keep one’s mouth shut,” much different than conventional tactics of “lowering voices.”383

Brennan’s opinion relied on the 1765 British case of Entick v. Carrington, which informed the “structure of the Fourth Amendment,” to maintain that “general search warrants are unlawful because of their uncertainty.”384 In Entick, John Entick sued three of the King’s messengers

379 Id.

380 Id. at 449 (Brennan, J., dissenting).


382 Lopez, 373 U.S. at 449 (Brennan, J., dissenting).

383 Id. at 453.

384 Id. at 454 (citing Entick v. Carrington, (1765) 19 How. St. Tr. 1029, 1066; 95 Eng. Rep. 807 (K.B.)). Entick v. Carrington was a case decided in 1765 and is the leading English law case for limiting the scope of executive power
who, under the authority of the secretary of state, had seized his personal papers that were
deemed seditious by the government. The seizure of the papers was made without a warrant.

Brennan said the “Warrant Clause” is a result of the American Revolution, spurred by the
“evil of the general warrant.”385 The general warrant gave the government the “untrammeled
right to extract evidence from people.”386 In this way, the Fourth and Fifth Amendments are
complementary and create a “comprehensive right of personal liberty in the face of governmental
intrusion.”387 Brennan said that American independence was born of this “one single factor”—
personal liberty.388

Justice Brennan also refers to the Boyd v. United States case, cited by Brandeis’ dissent in
Olmstead vs. United States, as an example of a decision that “has never been impeached.”389
The Boyd decision, as pointed out in the dissent, has been “repeatedly approved in the decisions
in order to protect the establishment of individual civil liberties. Entick involved three messengers of the British
King who, under the orders of the Secretary of State Lord Halifax, burglarized the home of John Entick, a writer.
They seized his private papers, which were found by the government to be seditious, and he was subsequently
arrested. The case was decided by the Chief Justice of the Common Pleas, Lord Camden, who held that the
secretary of state had no statutory right to order a warrant for seizure of the papers. Justice Camden reasoned that
citizens could do anything that was not forbidden by law, and conversely the state could only engage in actions,
which were permitted by law.

385 Lopez, 373 U.S. at 454 (Brennan, J., dissenting).
386 Id.
387 Id. at 455.
388 Id. at 454. “Historically we are dealing with a provision of the Constitution which sought to guard against an
abuse that more than any one single factor gave rise to American independence. John Adams surely is a competent
witness on the causes of the American Revolution. And he it was who said of Otis’ argument against search by the
police . . . ‘American independence was then and there born. Id. at 454 n. 3/6 (quoting 10 ADAMS, WORKS 247;
Harris v. United States, 331 U.S. 145 (1947) (Frankfurter, J., dissenting)). James Otis, Jr. was a Massachusetts
Advocate General of the Admiralty Court who in 1760 resigned after being asked to argue in favor of writs of
assistance. Otis decided instead, to represent the merchants in the case. In response to Otis’ 1761 argument for the
plaintiffs in court, John Adams said, "The child independence was then and there born,[for] every man of an
immense crowded audience appeared to me to go away as I did, ready to take arms against writs of assistance." See
also 2 LEGAL PAPERS OF ADAMS 106-47 (Wroth & Zobel, eds., 1965).
of the [c]ourt” and affirms a “comprehensive right of privacy, of individual freedom.”

Brennan asserts the “right to privacy” is a “basic constitutional right” that was upheld in *Mapp v. Ohio*, decided June 19, 1961. In *Mapp*, the U.S. Supreme Court held that the Fourth Amendment’s prohibition on search and seizure, as extended to the states through the Fourteenth Amendment, prohibited introducing illegally obtained information in criminal prosecutions.

Brennan’s dissent said that the *Olmstead* decision must be appraised against the backdrop of Boyd’s “liberal construction” of the Fourth and Fifth Amendments. The *Olmstead* decision held that no actual “trespass” and no seizure of “physical evidence” made the “Fourth Amendment inapplicable.” However, in *Olmstead*, the Court found telephonic communications to be “peculiar to wiretapping,” because telephone wires ran out of the home or office and were not part of it. Brennan said that “modern life” suggests that the telephone is just as valuable and “indispensable” in “free human communication” as the face-to-face home conversations of yesteryear. Brennan writes that the *Olmstead* decision, which controls electronic surveillance—“apart from wiretapping”—was “erroneously decided” because 1) *Olmstead* interprets the Fourth Amendment as “limited to the tangible fruits of actual trespasses,”—a departure from the *Boyd* case; 2) *Olmstead* is unsupportable because it only

---

390 “The authority of the *Boyd* decision has never been impeached. Its basic principle, that the Fourth and Fifth Amendments interact to create a comprehensive right of privacy, of individual freedom, has been repeatedly approved in the decisions of this Court . . . Thus we have held that the gist of the Fourth Amendment is ‘(t)he security of one's privacy against arbitrary intrusion by the police.’ *Lopez*, 373 U.S. at 456.

391 *Id.* at 456-57 (citing *Mapp v. Ohio*, 367 U.S. 643 (1961)).


393 *Lopez*, 373 U.S. at 457.

394 *Id.* at 457-58.

395 *Id.* at 458.

396 *Id.*
applies the Fourth Amendment to “problems familiar to the technology of the eighteenth century”—even though the Framers could not “foresee the invention of the telephone”; 3) Olmstead was not a “decisional revolution,” as the Court continued to follow the principles laid out in the Boyd decision; and 4) since Olmstead, the Court has undermined the “supports” for Olmstead’s interpretation of the Fourth Amendment, that “fruits of electronic surveillance though intangible, nevertheless are within the reach of the Amendment.”

Brennan’s dissent said a “search” occurs when a person “looks or listens,” not just when someone manually rummages concealed objects.” Still, Brennan’s dissent said that the Court has feared that “electronic surveillance” could never be reasonable within the meaning of the Amendment and furthermore, restrictions on electronic surveillance could strip law enforcement of a “useful technique” in criminal investigations.

Brandeis, in his dissenting opinion in Lopez, is careful to say that this does not mean that no search could be constitutionally devised, but that the requirements of the Fourth Amendment are “not inflexible.” Brandeis added that the Court must refuse to admit illegally-gathered

---

397 Id. at 458-60. Brennan’s phrase “tangible fruits of actual trespasses” is different than the Boyd holding because in Boyd, the Court said the federal act compelling the plaintiff to produce his financial books in court was unconstitutional under the Fourth Amendment—even though the compulsion did not involve an actual search or seizure. Boyd, 116 U.S. at 635.

398 Lopez, 373 U.S. at 458-60.

399 Id. at 463.

400 Justice Brennan explained:

But the argument is unconvincing. If in fact no warrant could be devised for electronic searches, that would be a compelling reason for forbidding them altogether. The requirements of the Fourth Amendment are not technical or unreasonably stringent; they are the bedrock rules without which there would be no effective protection of the right to personal liberty. A search for mere evidence offends the fundamental principle against self-incrimination, as Lord Camden clearly recognized; a merely exploratory search revives the evils of the general warrant, so bitterly opposed by the American Revolutionaries; and without some form of notice, police searches became intolerable intrusions into the privacy of home or office. Electronic searches cannot be tolerated in the name of law enforcement if they are inherently unconstitutional…But in any event, it is premature to conclude that no warrant for an electronic search can possibly be devised. The requirements of the Fourth Amendment are not inflexible, or obtusely unyielding to the legitimate needs of law enforcement. It is at least clear that ‘the procedure of antecedent justification before a magistrate that is
evidence in order to spur an “imaginative solution whereby the rights of individual liberty and
the needs of law enforcement are fairly accommodated.”

Brandeis said that just because “police traditionally engage in some rather disreputable practices of law enforcement is no
argument for their extension.”

Eavesdropping was indictable at common law and most of us would still agree that it is an unsavory practice. The limitations of human hearing, however, diminish its potentiality for harm. Electronic aids add a wholly new dimension to eavesdropping. They make it more
penetrating, more indiscriminate, more truly obnoxious to a free society. Electronic surveillance, in fact, makes the police omniscient; and police omniscience is one of the most effective tools of tyranny. ‘Eaves-droppers, or such as listen under walls or windows
or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at the court-leet: or are indictable at the sessions, and punishable by fine and finding sureties for their good
behaviour.’

“In the nature of things,” Brandeis added, “wiretapping is only useful in the investigation of crimes of a continuing nature, which are typically not major crimes… The same principles apply to electronic surveillance generally.” Brandeis said that electronic surveillance imports a peculiarly severe danger to the liberties of the person. To be secure against police officers' breaking and entering to search for physical objects is worth very little if there is no security against the officers' using secret recording devices to
purloin words spoken in confidence within the four walls of home or office. Our possessions are of little value compared to our personalities. And we must bear in mind that historically the search and seizure power was used to suppress freedom of speech and of the press… and that today, also, the liberties of the person are indivisible.

central to the Fourth Amendment could be made a precondition of lawful electronic surveillance. And there have been numerous suggestions of ways in which electronic searches could be made to comply with the other requirements of the Fourth Amendment. Id. at 464.

401 Id. at 465.

402 Id.


404 Lopez, 373 U.S. at 469.

405 Id. at 469-70.
Brandeis’ dissent said that electronic surveillance “strikes deeper than at the ancient feeling that a man’s home is his castle”; it “strikes at Freedom of communication.” Furthermore, freedom of speech is undermined where people fear to speak unconstrainedly in what they suppose to be the privacy of home and office. Brandeis said in dissent that the “right to privacy is the obverse of freedom of speech” in that the First Amendment freedoms can be seen to include “under certain circumstances” the right to anonymity.

The passive and the quiet, equally with the active and the aggressive, are entitled to protection when engaged in the precious activity of expressing ideas or beliefs. Electronic surveillance destroys all anonymity and all privacy; it makes government privy to everything that goes on. In light of these circumstances I think it is an intolerable anomaly that while conventional searches and seizures are regulated by the Fourth and Fourteenth Amendments and wiretapping is prohibited by federal statute, electronic surveillance as involved in the instant case, which poses the greatest danger to the right of private freedom, is wholly beyond the pale of federal law.

The majority opinion in Lopez struggled with the technological advances of the day, describing wiretapping as a “mechanical recording.” In Olmstead, the Court saw phone communication as a means of broadcasting private thoughts to the world, beyond the scope of Fourth Amendment privacy protections for home and property. The Lopez decision reinforced this reasoning, finding that Lopez opened up his private thoughts to search and seizure when he communicated them to another person. The concurring and dissenting opinions in Lopez represent a slightly modernized judicial view of developing telecommunications technology.

---

406 Under Hitler, when it became known that the secret police planted dictaphones in houses, members of families often gathered in bathrooms to conduct whispered discussions of intimate affairs, hoping thus to escape the reach of the sending apparatus. Id. at 470 (citing United States v. Lee, 193 F.2d 306, 317 (2d Cir. 1951) (dissenting opinion)). “Electronic surveillance strikes deeper than at the ancient feeling that a man's home is his castle; it strikes at Freedom of communication, a postulate of our kind of society. Lopez' words to Agent Davis captured by the Minifon were not constitutionally privileged by force of the First Amendment.” Id.

407 Id. (citing Donald B. King, Wire Tapping and Electronic Surveillance: A Neglected Constitutional Consideration, 66 DICK. L. REV. 17 (1961)).

408 Id.

409 Id. at 471.
Chief Justice Warren’s concurrence spoke of “fantastic advances in the field of electronic communication.” Justice Brennan’s dissent described the telephone as a “valuable” tool of modern human communication. These opinions would soon find footing in the Warren Court, which would overturn *Olmstead* and *Lopez*’s traditional interpretation of constitutional protection for the privacy of phone communications.

**Griswold v. State of Connecticut**

Following the *Lopez* decision, the Court would rule on a case involving contraceptives, decided on the issue of marital privacy. This *Griswold* case is significant because the U.S. Supreme Court reasoned that the Bill of Rights had implied “penumbras”, unspecified guarantees that are tangentially related to specifically named and protected rights. Specifically the right to privacy, although unnamed in the Constitution, emanated from other guarantees: The First Amendment right of association, the Third Amendment’s prohibition of quartering soldiers in any house during peacetime, The Fourth Amendment’s guarantee against unreasonable search and seizure and the Fifth Amendment’s privilege against self incrimination. This was the first time the Court recognized individual privacy rights. The “penumbra” reasoning in *Griswold* would quickly take hold in the Court and change the way that it viewed electronic communications.

*Griswold v. State of Connecticut*, decided June 7, 1965, (1965) involved defendants’ conviction for violating the Connecticut birth control law, which criminalized the use of contraceptives, and the subsequent appeal to the Sixth Circuit of the U.S. Court of Appeals. 410 The U.S. Supreme Court, in a 7-2 vote reversed the decision, finding the Connecticut law was unconstitutional because it intruded upon marital privacy. Justice Douglas wrote the majority

---

opinion, joined by Justices Warren, Clark, White, Brennan, Harlan and Goldberg. Justices Black and Stewart dissented. Although this is a case was decided primarily under the Ninth and Fourteenth Amendments, the Supreme Court clarified several issues of privacy of individuals and the home that are relevant in interpreting the Fourth Amendment’s protections. The Court said that the Bill of Rights provides guarantees that are related through penumbras.\(^{411}\)

Relying upon *Boyd v. United States*, the Court said these Penumbras create zones of privacy to protect against all government invasions into “the sanctity of a man’s home and the privacies of life.”\(^{412}\) Citing *Entick v. Carrington*, the majority said

> It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offense-it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment. Breaking into a house and opening boxes and drawers are circumstances of aggravation; but any forcible and compulsory extortion of a man's own testimony, or of his private papers to be used as evidence to convict him of crime, or to forfeit his goods, is within the condemnation of that judgment.\(^{413}\)

Justice Goldberg’s concurring opinion-- joined by Chief Justice Warren and Justice Brennan—added “I do agree that the concept of liberty protects those personal rights that are fundamental, and is not confined to the specific terms of the Bill of Rights.”\(^{414}\) Goldberg said, “The enumeration in the Constitution, of certain [Ninth Amendment] rights, shall not be construed to deny or disparage others retained by the people.” Justice Goldberg interpreted this

\(^{411}\) *Id.* at 484-85.

\(^{412}\) *Id.*. “The Fourth and Fifth Amendments were described in *Boyd v. United States* as protection against all governmental invasions ‘of the sanctity of a man's home and the privacies of life’ . . . We recently referred in *Mapp v. Ohio* to the Fourth Amendment as creating a ‘right to privacy, no less important than any other right carefully and particularly reserved to the people.’” *Id.* at 484 [citations omitted].

\(^{413}\) *Id.* at 484. *See also Entick v. Carrington*, (1765) 19 How. St. Tr. 1029, 1066; 95 Eng. Rep. 807 (K.B.) and *supra* notes 384-388.

\(^{414}\) *Id.* at 484.
Amendment, credited to James Madison, as a way to quiet fears that specifically enumerating rights would exclude rights not specifically mentioned. Madison said, ‘no language is so copious as to supply words and phrases for every complex idea.’ Goldberg quoted Madison in presenting the Amendment to demonstrate that the framers did not intend for the first eight amendments to be an exhaustive list of “basic and fundamental rights” constitutionally guaranteed to the people:

It has been objected also against a bill of rights, that, by enumerating particular exceptions to the grant of power, it would disparage those rights which were not placed in that enumeration; and it might follow by implication, that those rights which were not singled out, were intended to be assigned into the hands of the General Government, and were consequently insecure. This is one of the most plausible arguments I have ever heard urged against the admission of a bill of rights into this system; but, I conceive, that it may be guarded against. I have attempted it, as gentlemen may see by turning to the last clause of the fourth resolution (the Ninth Amendment).

Finally the “right of privacy” is recognized in the concurrence as a fundamental personal right “emanating ‘from the totality of the constitutional scheme under which we live.’” Citing Justice John Marshall Harlan II’s dissenting opinion in Poe v. Ullman, “Certainly the safeguarding of the home does not follow merely from the sanctity of property rights. The home derives its pre-eminence as the seat of family life. And the integrity of that life is something so fundamental that it has been found to draw to its protection the principles of more than one explicitly granted Constitutional right.”

---

415 Id. at 488 (Goldberg, J., concurring).
417 Griswold, 381 U.S. at 489-90 (Goldberg, J., concurring) (quoting 1 Annals of Cong. 439 (Gales ed. 1834)).
418 Id. at 494 (quoting Poe v. Ullman, 367 U.S. 497, 521 (1961) (Douglas, J., dissenting)).
419 Id. at 495 (quoting Poe v. Ullman, 367 U.S. 497, 551-52 (1961) (Harlan, J., dissenting)).
Berger v. New York

Following Griswold’s recognition of constitutional privacy rights, the Court would undergo a significant philosophical shift from its Olmstead and Lopez decisions on electronic surveillance. In the 1966 Ashton case, the Court had recognized the role of free discussion in civil and political discussions.420 In 1967, the Court would decide two cases that extended Fourth Amendment protections against warrantless search and seizure to phone communications.

In Ralph Berger v. State of New York, decided June 12, 1967, the defendant was convicted in a New York County Supreme Court on counts of conspiracy to bribe the chairman of the New York State Liquor Authority.421 The U.S. Supreme Court, in a 6-3 vote, held that conversations, in themselves, are protected by the Fourth Amendment, and capturing conversations through the use of electronic devices was a “search.”

The case involved a New York eavesdropping statute, which allowed the use of ex parte orders—general search warrants—to collect evidence, as long as an oath or affirmation was made that there was “reasonable ground” to believe that evidence of a crime “may” be obtained.422 The statute required that the oath or affirmation be made by: 1) the district attorney, 2) the attorney general or 3) an officer above the rank of sergeant of any police department of the state or any political subdivision thereof.423

Under the authority of the State Supreme Court, an order was issued permitting the installation, for a period of 60 days, of a recording device in the office of the defendant, a

---

420 Id. at 198-200.


422 Id.

423 Id. at 43-44.
suspected conspirator in a bribery ring involving the issuance of liquor licenses. The petitioner, Ralph Berger, was an attorney and a go between in this bribery operation. Berger objected to use of relevant portions of the recordings as evidence at trial. The recordings were played for the jury, and the verdict in the case upheld the constitutionality of the New York statute. 

Justice Clark wrote the majority opinion, which described eavesdropping as “an ancient practice, which at common law was condemned as a nuisance.” The telephone was described as a device that enabled a “more modern eavesdropper known as the wiretapper.” The Court said that wiretapping techniques—developed by science—have spurred lawmakers to create “statutory protection” against the “invasion of individual privacy.” The New York County Supreme Court decision, upholding the constitutionality of the statute was overturned, as the U.S. Supreme Court found the statute to be “offensive” based on four criteria:

I. The conversations were illegally obtained since the “property” sought was not “particularly described,” in keeping with the probable cause requirement of the Fourth Amendment. This illegal interception amounts to a “roving commission” to “seize any and all conversations” of the person targeted.

---

424 Id. at 44-45.
425 Id. at 45.
426 Id. at 45-47. “Sophisticated electronic devices have now been developed (commonly known as “bugs”) which are capable of eavesdropping on anyone in most any given situation. They are to be distinguished from “wiretaps,” which are confined to the interception of telegraphic and telephonic communications.” Id. at 46-47.
427 Id. at 46.
428 Id. at 47. “And the Founders so decided a quarter of a century later when they declared in the Fourth Amendment that the people had a right “to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” Indeed, that right, they wrote, ‘shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.’” Id. at 49. “The law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge. This is not to say that individual privacy has been relegated to a second-class position for it has been held since Lord Camden’s day that intrusions into [privacy] are ‘subversive of all the comforts of society.’” Id. at 49 (citing Entick v. Carrington, (1765) 19 How. St. Tr. 1029, 1066; 95 Eng. Rep. 807 (K.B.)).
429 Id. at 58-59.
II. The statute authorized a two-month period of eavesdropping on a 24-hour basis which would allow conversations to be “seized” with no “regard to their connection with the crime under investigation.” This coupled, with the statutory two-month extension made “in the public interest,” fails to meet requirements for probable cause.430

III. The statute does not specify a “termination date” for the eavesdropping, but instead places the termination at the discretion of the law enforcement officer conducting the surveillance.431

IV. The statute does not require notice, as do conventional warrants, because its “success depends on secrecy.” Nor does it require a “showing of exigent circumstances” to excuse this requirement. Therefore, there is no “judicial supervision or protective procedures.”432

The Supreme Court, in the Berger decision, said that it “cannot forgive the requirements of the Fourth Amendment in the name of law enforcement,” because the requirements are “basic to the privacy of every home in America.”433 Federal law enforcement officers must “comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded.”434 If this is not possible, the “fruits of eavesdropping devices are barred under the Amendment.”435

Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices. Some may claim that without the use of such devices crime detection in certain areas may suffer some delays since eavesdropping is quicker, easier, and more certain. However, techniques and practices may well be developed that will operate just as speedily and certainly and-what is more important-without attending illegality.436

430 Id. at 59.
431 Id. at 59-60.
432 Id. at 60.
433 Id. at 62-63.
434 Id. at 63.
435 Id.
436 Id.
The Court said that “under specific conditions and circumstances” eavesdropping devices are permissible if the “constitutional standard” is met before “official invasion is permissible.”\footnote{Id. at 63.}  

Justice William O. Douglas concurred in the Court’s majority opinion, particularly its “sub silentio” overruling of the \textit{Olmstead} decision.\footnote{Id. at 64 (Douglas, J., concurring). “Sub silentio” means without formal notice.}  He also condemned electronic surveillance for “its similarity to the general warrants out of which our Revolution sprang.”\footnote{Id. at 64-65.}

A discreet selective wiretap or electronic “bugging” is of course not rummaging around, collecting everything in the particular time and space zone. But even though it is limited in time, it is the greatest of all invasions of privacy. It places a government agent in the bedroom, in the business conference, in the social hour, in the lawyer's office-everywhere and anywhere a “bug” can be placed.\footnote{Id. at 64-65.}

Douglas said that a statute placing a policeman in every home or office would be struck down as a “bald invasion of privacy,” even if there were probable cause that evidence existed establishing a crime had been committed.\footnote{Id. at 67.}  He said that electronic surveillance creates a “dragnet” placing an “invisible policeman” in the home.\footnote{Id.}  This moves the country closer to a “totalitarian regime,” and further from the Fourth Amendment’s protection of privacy.\footnote{Id. at 68.}

Douglas argued for a “high constitutional barricade against the intrusion of Big Brother into the lives of all of us.”

Justice Potter Stewart, in his concurring opinion, said the state statute was constitutional because it did not authorize an unreasonable search and seizure. Its requirements were “more stringent than the Fourth Amendment,” with it’s “reasonable grounds” requirement” mirroring
“probable cause” under the Fourth Amendment.444 Stewart found the issue to be whether the statute’s search requirements meet Fourth Amendment standards—“showing of justification” must “match the degree of intrusion.”445 In this case, the judge was not presented with any facts to support the allegations against the target.

Justice Hugo Black dissented in the Berger opinion arguing that the Court’s decision makes it “completely impossible” for the state or the federal government to ever have valid eavesdropping statutes, because the Court negates New York’s criteria for probable cause for surveillance.446 Black was referring the majority opinion’s first criteria in evaluating the New York statute requiring that the property sought be “particularly described.”447 Black said that there is “no inherent danger” in using electronic recordings as evidence because they are “unerringly accurate” and therefore superior to oral testimony, which can be affected by memory and perspective.448 Black found it “impossible” that the “wise Framers of the Fourth Amendment” intended to protect the “right of privacy,” which he calls “a chameleon” that has a “different color for every turning.”449 He concluded that state legislatures should be free to pass laws about electronic surveillance—“Honest men may rightly differ on the potential dangers or benefits inherent in electronic eavesdropping and wiretapping.”450

444 Id. at 68-69 (Stewart, J., concurring in result).
445 Id. at 69.
446 Id. at 70-71 (Black, J., dissenting).
447 Id. at 58-59 (majority opinion).
448 Id. at 73 (Black, J., dissenting).
449 Id. at 77.
450 Id. at 88-89.
Justice Harlan dissented on the basis that the Court’s majority opinion violated the distinction between federal and state authority.\(^{451}\) He felt the decision would “thwart” Congressional efforts to refine the use of electronic eavesdropping as a law-enforcement” tool.\(^{452}\) Justice White dissented because he found the majority opinion would strike down the New York statute “on its face,” when there was no evidence that the petitioner’s constitutional rights had been violated.\(^{453}\) He said that the present case is not the “proper vehicle for resolving all of these broad constitutional and legislative issues raised by the problem of official use of wiretapping and eavesdropping.”\(^{454}\)

**Katz v. United States**

In *Charles Katz v. United States*, decided December 18, 1967, the U.S. Supreme Court held that the Fourth Amendment protection from unreasonable search and seizure protected individuals’ conversations in public telephone booths, specifically the use of warrantless wiretaps by authorities. Katz was convicted, in the United States District Court of Southern California, for the interstate transmission of bets or wagers by wire communications. Katz appealed, and the U.S. Court of Appeals for the Ninth Circuit affirmed the District Court’s decision and certiorari was granted “because there was no physical entrance into the area occupied” by Katz.\(^{455}\)

Justice Stewart wrote the majority opinion, joined by Chief Justice Warren and Justice Abe Fortas. Justice Douglas concurred, joined by Justice Brennan. Justice Harlan wrote a separate concurrence, as did Justice White. Justice Black wrote a dissenting opinion in the case. The

\(^{451}\) Id. at 89 (Harlan, J., dissenting).

\(^{452}\) Id.

\(^{453}\) Id. at 107.

\(^{454}\) Id. at 107.

Court, in its majority opinion, held that the government had no legal justification for electronically listening to and recording the defendant’s words over a telephone line in a public phone booth. Justice Stewart said the phone booth was a “search and seizure” zone for Fourth Amendment purposes and did not honor safeguards that kept it within constitutional standards.456

Katz raised two issues in his petition to the Court: 1) is a public telephone booth a constitutionally protected area in regards to “right to privacy” and “search and seizure” under the Fourth Amendment to the United States Constitution; and 2) is “physical penetration of a constitutionally protected area… necessary before a search and seizure can be said to be violative of the Fourth Amendment to the United States Constitution.”457 The Court declined “to adopt this formulation of the issues,” since the Fourth Amendment does not translate to a “general constitutional ‘right to privacy,’” instead it insures individual privacy against “certain kinds” of government intrusion.458 These intrusions are guarded against by the First Amendment—“limitations upon govermental abridgment of ‘freedom to associate and privacy in one's associations;’”459—The Third Amendment—“ prohibition against the unconsented peacetime quartering of soldiers protects another aspect of privacy from governmental intrusion;” and the Fifth Amendment—“the right of each individual ‘to a private enclave where he may lead a

456 Id.
457 Id. at 350-51.
458 “We decline to adopt this formulation of the issues. In the first place the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase ‘constitutionally protected area.’ Secondly, the Fourth Amendment cannot be translated into a general constitutional ‘right to privacy.’ That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion. But the protection of a person's general right to privacy-his right to be let alone by other people is, like the protection of his property and of his very life, left largely to the law of the individual States.” Id.
459 Id. at 351.
private life.”

“Virtually every governmental action interferes with personal privacy to some degree,” but the Court outlines the question in the case as when the action violates Constitutional Protections.

In *Katz*, the Court reasoned that what the petitioner sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

Although there was no physical penetration, the Court said that it departs from the narrow view of privacy in the *Olmstead* decision requiring actual trespass and seizure. As an example, the Court cited the *Silverman v. United States* case to show that they have found the Fourth Amendment to govern “recording of oral statements overheard without any ‘technical trespass under local property law.’”

The Court said that the controlling decisions of *Olmstead* and *Goldman* have been eroded and the “‘trespass doctrine’ no longer controls because electronic surveillance allows the government to engage in activities that constitute a search and seizure, without penetrating a wall. Therefore, the issue is whether the government agents followed the legal protocol to

460 Id. (citing Tehan v. United States ex rel. Shott, 382 U.S. 406 (1966)).
461 Id. at 350 (citing Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)).
462 Id. at 352 (citing Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920)).
463 Id.
464 Id. at 353 (citing Silverman v. United States, 365 U.S. 505 (1961)).
465 Id.
begin electronic surveillance—narrowly tailoring the activity and obtaining a warrant. The government did not attempt to attain judicial oversight of surveillance activities through a warrant, despite the fact, as the Court writes, one could have been obtained legally based on the facts of the case in light of past judicial examples. In regards to privacy considerations, Court found that they:

do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. The government agents here ignored ‘the procedure of antecedent justification that is central to the Fourth Amendment, 'a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case.'

Douglas concurred with the majority opinion and was joined by Justice Brennan, in making the important note that White’s concurring opinion was “a wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels ‘national security’ matters.” This could be problematic since the Executive Branch, unlike the Judicial Branch, is not “neutral or disinterested,” but charged with investigating crimes—sometimes ones in which they are the “intended victim.”

Justice Harlan also concurred with the majority opinion, but states that he relied upon the Silverman v. United States decision to emphasize that the “interception of conversations reasonably intended to private should constitute a ‘search and seizure’ and that the examination

466 Id. at 354.
467 Id.
468 Id. at 359.
469 Id. (Douglas, J., concurring).
470 Id. at 359-60.
or taking of physical property was not required.” 471 Silverman, in conjunction with the current case, were Harlan’s basis for arguing that the Goldman case should be reconsidered and overruled, “Its limitation on Fourth Amendment protection is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion.” 472

Justice Byron White concurred that the surveillance of a public phone booth was subject to warrant requirements, but found that previous cases were “undisturbed” by the current decision. 473 Also, White noted the Court’s acknowledgement that national security cases are beyond the reach of the current decision and can rely upon the considerations of the President of the United States or the Attorney General. 474

Justice Black dissented on the basis that 1) “the words of the Amendment will bear the meaning given them by today’s decision”; and 2) “the proper role of this Court” is not to rewrite the Amendment to “bring it into harmony with the times.” 475 Black elaborated to say the Fourth Amendment, through its first clause, protects “tangible things,” and through its second clause, protects those “tangible things” from search and seizure. 476 He said that the Court’s decision in this case would apply the Fourth Amendment to “overhearing future conversations which by their very nature are nonexistent until they take place.” 477 Therefore, it would be impossible to

471 Id. at 361-62 (citing Silverman v. United States, 365 U.S. 505 (1961)) (Harlan, J., concurring).
472 Id. at 362.
473 Id. at 362-63.
474 Id. at 363-64.
475 Id. at 364-65 (Black, J., dissenting).
476 Id. at 365.
477 Id.
obtain a warrant for a conversation that had simply been predicted to happen at some point in the future. He said—as the Court did in the Berger case—that applying the Fourth Amendment in this case—one of eavesdropping—is beyond the scope of what was envisioned by the Constitutional Framers:

Tapping telephone wires, of course, was an unknown possibility at the time the Fourth Amendment was adopted...In those days the eavesdropper listened by naked ear under the eaves of houses or their windows, or beyond their walls seeking out private discourse...There can be no doubt that the Framers were aware of this practice, and if they had desired to outlaw or restrict the use of evidence obtained by eavesdropping, I believe that they would have used the appropriate language to do so in the Fourth Amendment. They certainly would not have left such a task to the ingenuity of language-stretching judges. No one, it seems to me, can read the debates on the Bill of Rights without reaching the conclusion that its Framers and critics well knew the meaning of the words they used, what they would be understood to mean by others, their scope and their limitations.478

Black’s dissent was built on the premise that the Fourth Amendment, even with “liberal construction,” is “aimed directly at the abhorred practice of breaking in, ransacking and searching homes and other buildings and seizing people's personal belongings without warrants issued by magistrates.”479 He argued that Berger and the majority’s opinion in Katz were the cases to erode the doctrine established in Olmstead and Boyd, cases he continued to endorse.480

In Berger, the Court overturned the Olmstead holding, while at the same time recognizing the value of the telephone in promoting discourse among citizens. In doing so, the Court also recognized how the telephone facilitated eavesdropping—which the Court condemned in Berger on Fourth Amendment grounds.481 Previously, in Katz, the Court said only that the telephone had a vital role in private communication.482 This shift in the Court’s view of telephone

478 Id. at 366.
479 Id. at 366-67.
480 Id. at 367-72.
481 Id.
482 Katz, 389 U.S. at 352 (majority opinion) (citing Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920)).
communication—and its application of Fourth Amendment protections to electronic surveillance—was made possible by the *Griswold* Court’s recognition of a right to privacy in matters of private life.

In *Olmstead*, the Court recognized electronic surveillance as “mechanical recording.” In *Lopez*, Brennan’s dissent said the telephone was a valuable tool of human communication. Douglas’ concurrence in *Berger* went even further, likening warrantless surveillance to the general warrants used by the British against American colonists. Douglas uses powerful language in his concurrence suggesting that surveillance dragnets moved American closer toward a totalitarian regime. He even went so far as to draw a parallel between this type of government interception and the “Big Brother” regime of George Orwell’s novel, *Nineteen Eighty-Four*.

The Court’s updated view of phone communications and electronic surveillance would lead Congress to update the statutory framework for electronic surveillance. Following the *Berger* and *Katz* decisions, Congress, in 1968, passed the Omnibus Crime Control and Safe Streets Act, establishing a legal framework for federal authorities to obtain warrants for wiretapping in criminal investigations.

**United States v. United States District Court**

In *United States v. United States District Court* (hereinafter referred to as the Keith case), decided June 19, 1972, the U.S. Supreme Court, in an 8-0 decision, held that government officials must obtain a warrant before electronic surveillance is initiated in matters of domestic security. The United States asked the Supreme Court to compel the judge for the United

---

483 *Id.*

484 *United States v. United States District Court* is known as the “Keith Case” because Judge Damon Keith of the United States District Court for the Eastern District of Michigan—in a watershed decision—ordered the Government to disclose all illegally intercepted conversations to the defendants in the case.
States District Court for the Eastern District of Michigan to vacate an order directing the United States to make full disclosure of electronically monitored telephone conversations. The Government appealed the decision to the Court of Appeals for the Sixth Circuit, but the appeals court upheld the lower court decision. The U.S. Supreme Court granted a writ of certiorari in the case. Justice Lewis Powell, Jr. wrote the majority opinion of the Court affirming the appeals court decision. The majority in Keith held the Omnibus Crime Control and Safe Streets Act does not grant the president the power to conduct surveillance for purposes of national security and that “electronic surveillance in domestic security matters requires an appropriate prior warrant procedure.”

In the Keith case, the three defendants were charged with conspiracy to destroy government property. One of the defendants, Larry Plamondon, was charged with the bombing of a CIA office in Michigan. The Court said the issue in the case was whether the President had the power to authorize the Attorney General to conduct warrantless electronic surveillance in domestic security matters. Although, past Presidents had authorized this type of surveillance, it was the first time the issue—how to balance national security concerns and a citizen’s rights to privacy—came before the Supreme Court.

The defendants sought a hearing to force the government to disclose “certain electronic surveillance information.” The U.S. Attorney General, John Mitchell, responded with an affidavit that he had approved the wiretaps for the purpose of gathering intelligence information.

---

486 Id. at 298. Justice Rehnquist took no part in considering or deciding the case.
487 Id.
488 Id. at 299.
489 Id.
“necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government.” The surveillance logs were “filed in a sealed exhibit for in camera inspection by the district court.” The district court, relying on the affidavit and the logs, found the surveillance was unlawful because it was conducted without judicial approval. The government was ordered to disclose the logs to the defendant charged in the bombing. The government sought writ of mandamus from the U.S. Court of Appeals for the Sixth Circuit to “set aside the district court order.” The Supreme Court affirmed the Appeals Court decision.

In the Keith case, the Court majority found that the Omnibus Crime Control and Safe Streets Act authorized electronic surveillance for certain specifically named crimes, subject to prior court order. The Court held that the Act was a “comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression.” The Court acknowledged that the Omnibus Act was in part, a response to the Berger Case, which struck down a New York law that allowed authorized electronic surveillance without procedural safeguards. The Court cited Section 2511 (3) of the Omnibus Act, which states

Nothing contained in this chapter or Communications Act [citation omitted] of shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The

490 Id. at 300-01.
491 Id. at 301.
492 Id. at 301-02.
contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.493

The Government argued that 2511(3) empowered the President to authorize warrantless surveillance in cases of national security. The Court acknowledged that in passing the Act, Congress “recognized” the President’s authority to conduct warrantless surveillance of foreign powers, however the Court said that the language of the Act was neutral and conferred no power beyond what the President already enjoyed under the Constitution.494 The Court said that Congress did not intend to broaden the President’s power with the Omnibus Act, it meant only to preserve already existing powers.495 In contrast, the Court said, Section 2516 of the Omnibus Act governs executive-authorized surveillance, requiring the Attorney General to “make application to a federal judge” for surveillance. The Court’s majority opinion said Section 2518 of the Omnibus Act required prior approval, probable cause, “strict time limits” on surveillance and in “an emergency situation,” approval within 48 hours of interception of communications.496 The Court went further, to say, “Congress only intended to make clear that the Act simply did not legislate with respect to national security surveillances.”497 The Court used the legislative history to support the conclusion that Section 2511(3) was not the “measure of executive authority asserted in this case.” The Court said the Omnibus Crime Control and Safe Streets Act

493 Id. at 302-03.
494 Id. at 303.
495 Id.
496 Id. at 304-05.
497 Id. at 306.
raised a constitutional challenge.\textsuperscript{498} Although the Attorney General’s affidavit states the surveillance was necessary to “protect the nation from attempts of domestic organizations to attack and subvert the existing structure of Government,” the Court found there was no evidence of involvement by a foreign power in the conspiracy to bomb the CIA office.\textsuperscript{499} The Court said Section 2511(3) only authorizes Presidential power in cases where the national security is threatened by a foreign power.\textsuperscript{500} The President is charged with preserving protecting and defending the Constitution under Article II—and surveillance is an appropriate tool for carrying out this charge.\textsuperscript{501} However, citizen privacy must also be considered as a factor in national

\textsuperscript{498} Id. at 306-07. “Most relevant is the colloquy between Senators [Philip] Hart, [Spessard] Holland, and [John] McClellan [the Bill’s sponsor] on the Senate floor:

Mr. HOLLAND: The section (2511(3)) from which the Senator (Hart) has read does not affirmatively give any power. . . . We are not affirmatively conferring any power upon the President. We are simply saying that nothing herein shall limit such power as the President has under the Constitution . . . . We certainly do not grant him a thing. There is nothing affirmative in this statement.

Mr. MCCLELLAN: Mr. President, we make it understood that we are not trying to take anything away from him.

Mr. HOLLAND: The Senator is correct.

Mr. HART: Mr. President, there is no intention here to expand by this language a constitutional power. Clearly we could not do so.

Mr. MCCLELLAND: Even though intended, we could not do so.

Mr. HART: However, we are agreed that this language should not be regarded as intending to grant any authority, including authority to put a bug on, that the President does not have now. In addition, Mr. President, as I think our exchange makes clear, nothing in section 2511(3) even attempts to define the limits of the President’s national security power under present law, which I have always found extremely vague . . . . Section 2511(3) merely says that if the President has such a power, then its exercise is in no way affected by title III.”

\textit{Id.} (quoting 114 CONG. REC. 14751 (1968)).

\textsuperscript{499} Id. at 309.

\textsuperscript{500} Id.

\textsuperscript{501} “The coverture and complexity of potential unlawful conduct against the Government and the necessary dependency of many conspirators upon the telephone make electronic surveillance an effective investigatory instrument in certain circumstances. The marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission, and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its law abiding citizens.” \textit{Id.}, at 310-12.
security issues because the Bill of Rights safeguards the privacy of the home and private speech from “unreasonable surveillance.” Justice Powell, in the majority opinion, wrote that national security cases “reflect a convergence of First and Fourth Amendment values not present in cases of ‘ordinary’ crime,” with a “greater jeopardy to constitutionally protected speech.”

History abundantly documents the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect ‘domestic security.’ Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.

The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.

Therefore, the Court said that since the “Fourth Amendment is not absolute in its terms,” the biggest issue in the case is whether the government’s duty to protect national security outweighs constitutional protections for “individual privacy and free expression.” Essential to the decision was “whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it.” The Court said the Fourth Amendment requires judicial review of executive decisions in these cases because those charged with enforcing, investigating and prosecuting the law, “should not be the

For discussion of Article II, see infra.

502 Id. at 313.
503 Id.
504 Id. at 314.
505 Id. at 315.
506 Id. at 314-15.
507 Id. at 315.
sole judges of when to utilize constitutionally sensitive means in pursuing their tasks.”

Furthermore, “post-surveillance judicial review” does not safeguard Fourth Amendment rights in cases, which fail to result in prosecutions. The government’s belief that disclosure of information to a magistrate in these cases would jeopardize investigations does not justify a “departure from Fourth Amendment standards.”

If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.

The Court is careful to limit its decision to cases involving domestic aspects of national security, and not foreign powers or agents of foreign powers.

The Keith case was a landmark decision because it established the need for the government to obtain a warrant before electronic surveillance began in matters relating to domestic security. The Court said that the Omnibus Crime Control and Safe Streets Act did not give the President an unchecked power of surveillance in national security issues. The Keith case was the first time the Supreme Court considered the balance between national security concerns and constitutional protections for privacy. The Court, also for the first time, recognized that national security cases are unique in that they present a threat to constitutionally protected speech. The Court said the threat arose out of the convergence of First and Fourth Amendment issues.

---

508 Id. at 316-17.
509 Id. at 317-18.
510 Id. at 319-20.
511 Id. at 320.
512 Id. at 321-22.
513 Keith, 407 U.S. at 298.
The Court recognized that government attempts to protect domestic security had the potential to endanger “political dissent.” In contrast to the Court’s decisions on political dissent in *Schenck* and *Abrams*, the Keith decision offered some protection for unpopular political beliefs.\(^{514}\) Although the Court did not go so far as to directly recognize the value in these beliefs, it did decide the case on reasoning that reflect the marketplace of ideas model. The Courts language in discussing “unchecked surveillance power,” invokes the chilling effect doctrine when it says lawful public dissent must not be subject to “dread” from government action. It goes further in saying that the “fear” of unauthorized eavesdropping can “deter vigorous citizen dissent and discussion of Government action in private conversation.” The Court, in the Keith case, recognized the value of private dissent, not just public discourse.\(^{515}\) The Keith decision extended the marketplace of ideas, and its necessary breathing space, to private political dissent and association.

**California Bankers Association v. Shultz**

Two years after *Keith*, the U.S. Supreme Court would decide a case involving the government seizure of bank records. Although the case did not involve electronic surveillance, the reasoning in the opinion touched on First Amendment rights to associational privacy. Justice Douglas’ dissent in the case relied upon the *Katz* and *Keith* decisions and hinted at a future where all electronic records might be subject to search and seizure by the government.

In *California Bankers Association v. Shultz*, decided April 1, 1974, the Supreme Court, in a 6-3 vote, held that regulations requiring banks to keep records and report them to the Secretary of the Treasury did not constitute a Fourth Amendment seizure, nor did it violate the members’

\(^{514}\) *Id.* at 314.

\(^{515}\) *Id.* at 315.
First Amendment rights to association.\textsuperscript{516} The regulation in question was the Bank Secrecy Act of 1970, that required banks to keep and report records with “a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings.”\textsuperscript{517}

Justice Rehnquist wrote the majority opinion joined by Justices Burger, Steward, White, Blackmun, and Powell. Justices Douglas, Brennan and Marshall dissented. The Court found that the statute did not violate the Fourth Amendment rights of the plaintiffs in requiring information be disclosed to the government.\textsuperscript{518} The plaintiffs argued that the bank acted as an “agent of the Government” in keeping records and reporting them pursuant to the act, but the Court said this was not a search and seizure because in all of the transactions the bank was “itself a party.”\textsuperscript{519} Also, the banks “voluntarily kept records” before required to by regulation, so the records were useful to the bank in its own business practices.\textsuperscript{520}

In regards to the Schultz’s claim that the recordkeeping requirements violated the members First Amendment rights, the Court found that there was no threat to associational privacy.\textsuperscript{521} This Court said this was because the threat was remote and different than the previous cases decided on this issue, including: 1) \textit{Laird v. Tatum}—where the records of the Army’s system were less remote; \textsuperscript{522} 2) \textit{Boyd v. United States}—where a foreign reporting requirement was found


\textsuperscript{517} \textit{Id}.

\textsuperscript{518} \textit{Id}. at 52.

\textsuperscript{519} \textit{Id}. (citing United States v. Biswell, 406 U.S. 311 (1972)).

\textsuperscript{520} \textit{Id}. at 53.

\textsuperscript{521} \textit{Id}. at 56-57.

\textsuperscript{522} The \textit{Laird} case involved a general contingency plan developed by the Department of the Army to assist local authorities in “quelling” Detroit, Michigan civil disorder. In \textit{Laird}, decided June 26, 1972 in a 5-4 vote, the Supreme Court held that the plan did not “constitute a justifiable controversy on the basis of the record in this case, disclosing as it does no showing of objective harm or threat of specific future harm.” Laird v. Tatum, 408 U.S. 1 (1972).
invalid under the Fourth Amendment as a general warrant;\textsuperscript{523} and 3) \textit{Stanford v. Texas}—where regulations were found to be “obnoxious to the Fourth Amendment.”\textsuperscript{524} The Court deferred to the judgment of Congress when it passed the 1970 Bank Secrecy Act provisions under challenge, and said the fact that a legislative enactment manifests a concern for the enforcement of the criminal law does not cast any “generalized pall of constitutional suspicion” over it.\textsuperscript{525}

Justice Douglas, in his dissent, called attention to the nature of the records at hand suggesting that

It would be highly useful to governmental espionage to have like reports from all our bookstores, all our hardware and retail stores, all our drugstores. These records too might be ‘useful’ in criminal investigations. One's reading habits furnish telltale clues to those who are bent on bending us to one point of view. What one buys at the hardware and retail stores may furnish clues to potential uses of wires, soap powders, and the like used by criminals. A mandatory recording of all telephone conversations would be better than the recording of checks under the Bank Secrecy Act, if Big Brother is to have his way. The records of checks-now available to the investigators-are highly useful. In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum. These are all tied to one's social security number; and now that we have the data banks, these other items will enrich that storehouse and make it possible for a bureaucrat-by pushing one button-to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates.\textsuperscript{526}

Douglas added that it would be “sheer nonsense” to agree that all citizen’s bank records have a “high degree of usefulness in criminal, tax, or regulatory investigations or proceedings,”


\textsuperscript{524} The \textit{Stanford} case involved the Texas Suppression Act of 1955, which outlawed the Communist party and created criminal offenses for Communist party association. \textit{Stanford v. Texas}, 379 U.S. 476 (1965). See also \textit{TEX. REV. CIV. STAT. ANN.} art. 6889-3A, § 2 (Vernon 1957) (repealed 1993). A Texas District Court Judge issued a warrant for the search of the petitioner’s home. The four-hour search by federal officers resulted in the seizure of over 2000 items, none of which were Communist-related. Stanford filed a motion for the return of the seized items, but the motion was denied by the Fifty-seventh Judicial Court of Texas. In \textit{Stanford}, decided January 18, 1965, the Supreme Court, in a 9-0 vote, extended Fourth Amendment protections through the Fourteenth Amendments to constitutionally bar states from issuing general search warrants.


\textsuperscript{526} Id. at 84-85 (Douglas, J., dissenting).
and doing so amounts to assuming that “every citizen is a crook.” He said that if the “religion, ideology, opinions, and interests,” of each citizen are “automatically” available to federal agencies, that it would be a “sledge-hammer approach to a problem that only a delicate scalpel can manage.”

He added that he was “not yet ready to agree that America is so possessed with evil that we must level all constitutional barriers to give our civil authorities the tools to catch criminals.”

Douglas, relying upon the idea of privacy that he outlined in his concurring opinion in *Katz*, said that “bank accounts are within the ‘expectations of privacy’ category,” because they reflect a person’s “interests, his debts, his way of life, his family, and his civic commitments.”

Unrestricted access by government agents to the bank records would be an unwarranted search, and as in the Keith case, this holds the potential for “invasion of privacy and protected speech.” Douglas’ dissent then takes a prophetic turn as he compares bank records to phone communications, and predict future requests by Congress

Suppose Congress passed a law requiring telephone companies to record and retain all telephone calls and make them available to any federal agency on request. Would we hesitate even a moment before striking it down? I think not, for we condemned in United States v. United States District Court ‘the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails.’

Douglas then said the Bank Secrecy Act gave Congressional authority to the Secretary of the Treasury to conduct warrantless surveillance, a move that he said would represent a “slow

---

527 Id. at 85.
528 Id.
529 Id. at 86.
530 Id. at 80.
532 Id.
533 Schultz, 416 U.S. at 89-90 (Douglas, J., dissenting).
eclipse of Congress by the mounting Executive power.”

Douglas’ dissent makes clear that he sees the banking records Act as a search and seizure under the Fourth Amendment. He quotes Justice Bradley’s word in the majority opinion for the *Boyd* case

> It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure.

Douglas also highlighted the nature of intangible property with regards to search and seizure as laid out in *Katz v. United States*, since the members disclosed information to the bank “for a limited purpose” within the “context of a confidential relationship.” In regards to the majority’s opinion in *Schulz*—that the Act only required record keeping and did not change the law regulating “acquisition of records by the government”—Douglas said that “this attempt to bifurcate the acquisition of information into two independent and unrelated steps is wholly unrealistic.” He added that the record keeping requirement “feeds into a system of widespread informal access to bank records by Government agencies and law enforcement personnel.”

Finally, he said that although bank records might be used as “negotiable instruments for illegal purposes,” this alone “cannot justify the Government's running roughshod over the First Amendment rights of the hundreds of lawful yet controversial organizations.”

---

534 *Id.* at 90-91.
535 *Id.* at 94.
536 *Id.*
537 *Id.* at 95-96 (citing *Katz v. United States*, 389 U.S. 347, 512 (1967)).
538 *Id.* at 96-97.
539 *Id.* at 99.
Justice Douglas, in the mid-1970’s could not have foreseen the amazing technological revolution that was about to occur in regards to telecommunications and computer technology. His dissent, however, evokes scenarios that have become contemporary reality. The PATRIOT Act allows federal officials to access “reports from all our bookstores, all our hardware and retail stores, all our drugstores.” The Act also allows the monitoring of bookstore purchases and library accounts.

The Terrorist Surveillance Program is still under judicial review, but as will be discussed in Chapter Four, it may be possible for the government to record “all telephone conversations.” Douglas theorized that Congress could pass a law requiring telephone companies to record and retain telephone calls for the federal government. Twenty years after his prediction, Congress passed CALEA requiring telecommunication carriers to build in government access for electronic surveillance.

Zweibon v. Mitchell

Just three years after the Keith decision, a District Court case was decided that challenged the Supreme Court’s landmark holding. Keith had established a need for warrants before the government could begin electronic surveillance in domestic security investigations, but it left open the question of how domestic investigations should be handled when the conspirators were engaged in activities related to foreign security. In *Bertram Zweibon, et al. v. John N. Mitchell*, decided June 23, 1975, the United States District Court of Columbia held that the President did have the power to authorize warrantless surveillance in domestic matters relating to the foreign aspects of national security.

In *Zweibon*, the New York headquarters of a political organization, demonstrating against the Attorney General’s Soviet policy, was the target of electronic surveillance by the Federal
Bureau of Investigations.\textsuperscript{540} The plaintiffs were 16 members of the Jewish Defense League and the defendants were Attorney General John Mitchell and agents and employees of the FBI.\textsuperscript{541} The plaintiffs brought suit under Title 18 U.S. Code §§ 2510-2520 for damages imposed by that statute resulting from alleged unlawful electronic surveillance overhearings of plaintiffs' telephone conversations during the month of October, 1970 and from January 5, 1971 through June 30, 1971.\textsuperscript{542} The Attorney General believed that at least some of the activities of the Jewish Defense league were “obviously detrimental to the continued peaceful relations between the United States and the Soviet Union and threatened the President's ability and constitutional authority to conduct the foreign relations of this country.”\textsuperscript{543}

The district court judge in \textit{Zweibon} held that the organizations activities threatened peaceful relations with the Soviet Union and endangered the lives of Americans in Moscow. Furthermore, court authorization for the electronic surveillance was unnecessary because of the foreign nature of the target’s activities. The President was found to have constitutional power to authorize the surveillance.\textsuperscript{544} The court found that the FBI’s surveillance was a “proper exercise of the President's constitutional authority to conduct the nation's foreign relations and his power to protect the national security,” and beyond the reach of the Omnibus Crime Control and Safe Streets Act.\textsuperscript{545}


\textsuperscript{541} \textit{Id.}

\textsuperscript{542} \textit{Id.}

\textsuperscript{543} \textit{Id.} at 937-43.

\textsuperscript{544} 18 U.S.C.A. §§ 2510-2520, 2511(3).

\textsuperscript{545} “The pertinent part of Section 2511(3) provides:

Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1103; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to
The district court made clear that Congress had intended to remain neutral on the President’s national security powers, as outlined by the decision in the Keith case, which found Title III did not apply to national security surveillance by the executive.546 However, the Jewish Defense League “posed a threat to the continuance of our peaceful foreign relations with the Soviet Union and subjected American citizens living in Moscow to harm by retaliation.”547 The Court said this threat to foreign relations brought the surveillance under the authority of the executive, not the judiciary.548 The Court found that no prior judicial authorization is necessary when electronic surveillance is conducted in relation to “foreign aspects” of national security.549

Three years later, Congress would pass the Foreign Intelligence Surveillance Act of 1978 to provide a statutory framework for obtaining surveillance warrants in foreign intelligence investigations.

obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial, hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power. Zweibon, 363 F. Supp. at 942 (citing Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510-2520).

546 Id. at 942-43.
547 Id. at 943.
548 Id.
549 Id.
CHAPTER 4
CONTEMPORARY ISSUES

This chapter will explore the contemporary legislative, executive and judicial actions involving the Terrorist Surveillance Program. First, government and industry reports of technological advancements in the telecommunications industry will be examined to the extent they influence electronic surveillance. Then, the Terrorist Surveillance Program, a warrantless domestic surveillance program authorized by the Bush Administration, will be introduced and explained. Finally, court cases filed in response to the Terrorist Surveillance Program will be introduced and explained, providing their current status in the judicial system.

**Technological Transition**

In 2001, before the September 11th attacks, the National Security Agency provided the incoming Bush Administration with the “Transition 2001” report.¹ The report, which was originally classified because it contained communications intelligence information, was prepared to provide the new president with background information on the National Security Agency’s mission, structure, focus and budget.² The report said analog communications were being replaced by digital data, prompting the NSA to recommended the government establish a “permanent presence on a global telecommunications network” to protect domestic communications and target adversarial communications.³

---


³ In the past, NSA operated in a mostly analog world of point-to-point communications carried along discrete, dedicated voice channels. These communications were rarely encrypted, and those that were used mostly indigenous encryption that did not change frequently. Before the arrival of fiber optic technology, most of these communications were in the air and could be accessed using conventional means; the volume was growing but at a rate that could be processed and exploited. Id. at 31.
report, said that “tailored access” would be necessary to facilitate this cooperation with partners.4
The report said the NSA was prepared to “exploit in an unprecedented way the explosion in
global communications.”5

In the Transition 2001 report, the NSA “demands a policy recognition that [it] will be a
legal but also a powerful and permanent presence on a global telecommunications infrastructure
where protected American communications are targeted adversary communications will
coexist.”6 The NSA, in the report, said that the “volume, velocity, and variety of information”
currently on global networks “demands a fresh approach to the way NSA has traditionally done
business.”7

The report suggested that the Information Age “may” require a “restatement and
endorsement” of the NSA’s Industrial Age policies.8 It is not clear what this statement means—
as there is no elaboration on the point—but the report immediately emphasized that global
networks of the 21st century have made gaining access to communications more difficult.9 The
NSA, in the report, added that the Information Age might also cause the agency to “rethink and
reapply the [Fourth Amendment] procedures, policies and authorities born in an earlier electronic
surveillance environment.”10 The report reiterated the NSA’s commitment to the Fourth
Amendment, but says that “senior leadership must understand that today’s and tomorrow’s
mission will demand a powerful, permanent presence on a global telecommunications network

4 Id. at 3.
5 Id. at 31.
6 Id.
7 Id. at 32.
8 Id.
9 Id.
10 Id.
that will host the “protected” communications of Americans as well as the targeted communications of adversaries.”\(^{11}\) Given that the document was classified, the Bush administration made no official statement regarding the report. However, in a speech on March 26, 2004, President George W. Bush recognized two Information Age factors driving the explosive growth in the telecommunications market: technology and competition.\(^{12}\) He also set a “national goal for… the spread of broadband technology” by 2007.\(^{13}\)

Two events have significantly shaped the telecommunications industry and reflect technological changes and competitive forces, identified by President Bush: 1) the 1984 breakup of the American Bell Telephone monopoly and 2) The Telecommunications Act of 1996. The American Telephone and Telegraph Company (AT&T) incorporated in 1885 as part of the parent company American Bell Telephone Company.\(^{14}\) In 1899, AT&T acquired American Bell’s assets and became known as the Bell Telephone System.\(^{15}\) AT&T is primarily concerned with networking, the interconnection of cables and fibers, which carry phone and other communication transmissions.\(^{16}\) The network is primarily comprised of three components: 1) “transmission,” which involves the routes over which the messages travel, 2) “switching,” which

---

\(^{11}\) Id.


\(^{13}\) Id.

\(^{14}\) AT&T Milestones in History, http://att.de/history/milestones.html (last visited June 22, 2008). The original corporate charter said the company’s mission was to “connect one or more points in each and every city, town or place in the State of New York with one or more point in every other city, town or place in said State and in each and every other of the United States, Canada and Mexico; and each and every of said cities, towns and places is to be connected with each and every other city, town or place in said states and countries, and also by cable and other appropriate means with the rest of the known world.” JONATHAN E. NEUCHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS (2005).


\(^{16}\) Id.
involves the systems for routing messages, and 3) management,” which involves the “intelligence” that makes the system function.\textsuperscript{17}

The Bell System officially ceased to exist on January 1, 1984, after a 1982 agreement was reached between AT&T and the U.S. Justice Department.\textsuperscript{18} The agreement, in response to a 1974 anti-trust suit, resulted in AT&T agreeing to “divest itself of local telephone operations.”\textsuperscript{19} The Bell system was split into seven Regional Bell Operating Companies and AT&T retained “long distance telephone, manufacturing, and research and development operations.”\textsuperscript{20} The split of the Bell system was intended to promote competition and encourage development of the telecommunications system.

A little more than a decade after the breakup of AT&T, Congress passed The Telecommunications Act of 1996 to address technological convergence, open telecommunications markets and foster competition.\textsuperscript{21} The changes brought about by converging landline, wireless and broadband technologies were possible in large part thanks to expanding technology. As National Security Agency Director Michael Hayden highlighted, in his 2002 statement to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, the convergence of these technologies has resulted in a situation where the government is increasingly reliant upon the telecommunications industry to carry our

\textsuperscript{17} \textit{Id.}


\textsuperscript{19} AT&T Milestones in History, \url{http://att.de/history/milestones.html} (last visited June 22, 2008).

\textsuperscript{20} \textit{Id.}

electronic surveillance. Hayden said that commercial broadband carries the bulk of communications in the United States. These telecommunication carriers also contract with the government for outsourcing. An example of this is the “Groundbreaker” program, which outsources information technology necessary to serve the mission of the NSA. Groundbreaker is an effort to modernize the NSA’s electronics infrastructure through a contract with the private Computer Sciences Corporation, a company that leases electronic equipment to the NSA for use in surveillance.

In his 2002 statement to the Intelligence committees, Hayden said he had met with “prominent corporate executive officers” to discuss the NSA’s data management needs. Hayden briefly discussed the “Trailblazer program” and how the government had awarded the contract to a private firm. Trailblazer improves signals intelligence (SIGINT) gathering by replacing outdated Cold War technology with information technology that can handle the “surveillance [and analysis] of cell phones, e-mail, fiber-optic telephones and other modern communication technologies.” Hayden also mentioned an unnamed program that enlisted a “corporate giant to jointly develop a system to mine data that helps us learn about our

---


24 Id.

25 Hayden Statement, supra note 22.

26 Id.


28 Id. See also Lipowicz, supra note 27.
Hayden said that the NSA spent about a third of its budget “making things ourselves.” He said that number would be down to 17% by 2003. The relationship between the government and private corporations was well documented through Hayden’s specification of contracts and programs.

**The Terrorist Surveillance Program**

President George Bush declared a War on Terror in 2001 after the attacks on the World Trade Center. In a speech to Congress on September 20, 2001, just days after the attacks, President George W. Bush addressed the growing national fear of terrorism by saying that terrorist were the “heirs of all the murderous ideologies of the 20th century… sacrificing human life to serve their radical visions.”

On October 26, 2001, Congress passed the USA PATRIOT Act, modifying the Foreign Intelligence Surveillance Act, and expanding the government’s wiretapping powers. U.S. citizens could now be targeted in foreign intelligence surveillance, as long as they were not engaged in First Amendment activities. The PATRIOT Act extended FISA surveillance procedures to the crime of terrorism. The PATRIOT Act gave federal intelligence agencies powerful new tools to protect national security, including: sharing information between agencies, allowing roving wiretaps to track mobile targets using wireless communication technology and

---

29 Hayden Statement, *supra* note 22.

30 *Id.*

31 *Id.*

32 Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11, 2 PUB. PAPERS 1140 (Sept. 20, 2001).

33 *Id.*

delaying target notification of surveillance warrants. Since the passage of the PATRIOT Act, scholars have questioned how the modification affects citizens’ constitutional privacy rights.\(^3\)

In 2002, President Bush issued a secret order authorizing the Terrorist Surveillance Program as a tool to fight the War on Terror.\(^3\) This order sidestepped a long-standing requirement of FISA that required federal authorities to obtain a warrant when wiretapping a United States citizen.\(^3\) The Terrorist Surveillance Program was a domestic wiretapping program


\(^3\) “You know, we feel comfortable that this surveillance is consistent with requirements of the 4th Amendment. The touchstone of the 4th Amendment is reasonableness, and the Supreme Court has long held that there are exceptions to the warrant requirement in -- when special needs outside the law enforcement arena. And we think that that standard has been met here. When you're talking about communications involving al Qaeda, when you -- obviously there are significant privacy interests implicated here, but we think that those privacy interests have been addressed; when you think about the fact that this is an authorization that's ongoing, it's not a permanent authorization, it has to be reevaluated from time to time. There are additional safeguards that have been in place -- that have been imposed out at NSA, and we believe that it is a reasonable application of these authorities. (Gonzales)

The President, of course, is very concerned about the protection of civil liberties, and that's why we've got strict parameters, strict guidelines in place out at NSA to ensure that the program is operating in a way that is consistent with the President’s directives. And, again, the authorization by the President is only to engage in surveillance of communications where one party is outside the United States, and where we have a reasonable basis to conclude that one of the parties of the communication is either a member of al Qaeda or affiliated with al Qaeda. (Gonzales)

Across the board, there is a judgment that we all have to make -- and I made this speech a day or two after 9/11 to the NSA workforce -- I said, free peoples always have to judge where they want to be on that spectrum between security and liberty; that there will be great pressures on us after those attacks to move our national banner down in the direction of security. What I said to the NSA workforce is, our job is to keep Americans free by making Americans feel safe again. That's been the mission of the National Security Agency since the day after the attack, is when I talked -- two days after the attack is when I said that to the workforce.

There's always a balancing between security and liberty. We understand that this is a more -- I'll use the word "aggressive" program than would be traditionally available under FISA. It is also less intrusive. It deals only with international calls. It is generally for far shorter periods of time. And it is not designed to collect reams of intelligence, but to detect and warn and prevent about attacks. And, therefore, that's where we've decided to draw that balance between security and liberty. (Hayden)


managed by the National Security Agency.\textsuperscript{38} The purpose of the Terrorist Surveillance Program—as the name implies—was to detect conspiratory communications between U.S. citizens and individuals with terrorist connections in other countries.\textsuperscript{39} The Bush administration said the Terrorist Surveillance Program was a means to address emergent national security concerns and issues related to terrorism.\textsuperscript{40}

After the \textit{New York Times} article revealed the existence of the Terrorist Surveillance Program, the Bush Administration immediately tried to assure the public that measures were taken to ensure both the legality and necessity of the surveillance program. In a radio address on December 17, 2005, Bush acknowledged the existence of the orders he signed authorizing the program.\textsuperscript{41}

In the weeks following the terrorist attacks on our nation, I authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with- (A) a court order directing such assistance signed by the authorizing judge, or (B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required.

For a full discussion of FISA, see \textit{supra} Chapter 2.

\textsuperscript{38} Risen & Lichtblau, \textit{supra} note 5. In December of 2005, Congress met to negotiate extending the powers of the USA PATRIOT Act of 2001, a statute largely concerned with demolishing the historical wall between intelligence and law enforcement.

\textsuperscript{39} President’s Radio Address, 41 \textit{WEEKLY COMP. PRES. DOC.} 1880 (Dec. 17, 2005). \textit{See also} Risen & Lichtblau, \textit{supra} note 5.

\textsuperscript{40} Risen & Lichtblau, \textit{supra} note 5.

\textsuperscript{41} President’s Radio Address, 41 \textit{WEEKLY COMP. PRES. DOC.} 1880 (Dec. 17, 2005).
organizations. Before we intercept these communications, the government must have information that establishes a clear link to these terrorist networks.42

Bush, in his radio address, described the TSP as “a highly classified program that is crucial to our national security.”43 He said the purpose of the TSP was “to detect and prevent terrorist attacks against the United States, our friends and allies.”44

On December 19, 2005, just two days after Bush’s radio address to the American people, Attorney General Alberto Gonzales appeared at a press conference to assure Americans that the President was justified in his actions by his “inherent Presidential powers” and the 2001 Congressional Authorization to Use Military Force in the War on Terror.45 The inherent powers of the President are based on Article II of the Constitution, which requires the President to take the following oath upon assuming office:

I do solemnly swear (or affirm) that I will faithfully execute the Office of President of the United States, and will to the best of my Ability, preserve, protect and defend the Constitution of the United States.46

This oath, specifically to “preserve, protect and defend” the United States Constitution charges the President with the legal responsibility to protect against foreign attack. Said this duty legally supported the use of warrantless domestic to stop terrorist attacks.47

The Authorization for Use of Military Force (hereinafter AUMF), a joint-congressional resolution, was signed on September 18, 2001, in response to the September 11th terrorist attacks

42 Id.
43 Id.
44 Id.
45 See Gonzales & Hayden Press Briefing, supra note 36.
46 U.S. CONST. art. II, § 1.
47 See Gonzales & Hayden Press Briefing, supra note 36.
on “the United States and its citizens.” In the AUMF, Congress recognized the national right to “self-defense” in protecting U.S. citizens from “grave acts of violence.” The AUMF recognized the President’s Constitutional authority to “take action to deter and prevent acts of international terrorism against the United States,” as long as there was an “unusual and extraordinary threat to the national security and foreign policy of the United States.”

Section 2(a) of the Authorization for Use of Military force says:

The President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

Attorney General Gonzales, in the press conference, said:

Now, in terms of legal authorities, the Foreign Intelligence Surveillance Act ... requires a court order before engaging in this kind of surveillance that I’ve just discussed and the President announced on Saturday ... unless otherwise authorized by statute or by Congress. That's what the law requires. Our position is, is that the authorization to use force, which was passed by the Congress in the days following September 11th, constitutes that other authorization, that other statute by Congress, to engage in this kind of signals intelligence.

Gonzales highlighted the “special needs” created by terrorism in regards to warrant requirements, upholding the constitutionality of the Terrorist Surveillance Program.

You know, we feel comfortable that this surveillance is consistent with requirements of the 4th Amendment. The touchstone of the 4th Amendment is reasonableness, and the Supreme Court has long held that there are exceptions to the warrant requirement in -- when special needs outside the law enforcement arena. And we think that that standard has been met here.

---

49 Id. at § 2(a).
50 See Gonzales & Hayden Press Briefing, supra note 36.
51 Id.
Gonzales added that although there was a “significant privacy interest” in protecting communications, but the temporary nature of warrantless surveillance authorization under the TSP provided adequate safeguards. Gonzales said President Bush was “very concerned about the protection of civil liberties” and that is why the TSP only authorized warrantless surveillance when “one party is outside the United States” or there was a “reasonable basis to conclude that one of the parties of the communication is either a member of al Qaeda or affiliated with al Qaeda.”

In the same press conference, Principal Deputy Director for National Intelligence Michael Hayden, said that “there's always a balancing between security and liberty,” but the administration had upheld the balance by limiting the reach of the Terrorist Surveillance Program. Hayden said

We understand that this is a more…aggressive program than would be traditionally available under FISA. It is also less intrusive. It deals only with international calls. It is generally for far shorter periods of time. And it is not designed to collect reams of intelligence, but to detect and warn and prevent about attacks.

On February 6, 2006, Attorney General Gonzales defended the constitutionality of the Terrorist Surveillance program to the Senate Judiciary Committee, describing the program as an early warning system for the twenty-first century. Gonzales described al Qaeda as an unconventional enemy with sophisticated communications, requiring the U.S. government to rely

52 Id.
53 Id.
54 Id.
on its technological strengths to prevail in the War on Terrorism.\textsuperscript{56} He also stated that the current program has a stronger focus than past presidential surveillance initiatives and is necessary to protect cherished civil liberties.\textsuperscript{57}

Little is known about the Terrorist Surveillance Program, as the order authorizing it is “secret” and the government has withheld details of the program under “state privilege.”\textsuperscript{58} What is known about the program comes from media reports relying on interviews with anonymous sources within the intelligence community. Two anonymous U.S. intelligence officials outlined the Terrorist Surveillance Program in a February 2006 \textit{USA Today} story, revealing how decisions to monitor calls are made.\textsuperscript{59} The intelligence officials said a forty-eight-point checklist was used to determine if the target has links to al-Qaeda or there is some other “reasonable basis” for suspecting terrorist activities.\textsuperscript{60} In his December 19, 2005 press conference, Attorney General Gonzales said that the Terrorist Surveillance Program only authorized surveillance in cases where there was a “reasonable basis” to believe that one of the targets was either outside of the

\begin{footnotesize}
\begin{enumerate}
\item Id.
\item Id. Jason A. Gonzalez, \textit{Constitutional Aspects of Foreign Affairs: How the War on Terrorism Has Changed the Intelligence Gathering Paradigm}, 51 NAVAL L. REV. 289 (2005). Jason Gonzalez (no relation to the Attorney General Gonzales) provides a congressional, executive and judicial history of FISA in his article, and examines the law’s background through the scope of a changing intelligence paradigm. He says that the pendulum shifts during wartime and Congress should not unduly restrain the President’s power to conduct defensive wars. Gonzalez leans on historical examples, such as President Roosevelt’s 1940 memorandum approving electronic domestic surveillance to prevent subversive activities against the government. He also cites the use of warrantless surveillance in the early 1950s national security context as a means to expose subversive communist activities. The author, Gonzalez concludes by saying the President has a “broad power to redirect his national security forces inward.”
\item See supra text accompanying note 205 for the definition of state secret privilege.
\item Leslie Cauley & John Diamond, \textit{Telecoms let NSA spy on calls}, USA TODAY, Feb. 6, 2006, available at http://www.usatoday.com/news/washington/2006-02-05-nsa-telecoms_x.htm?POE=NEWISVA. To date, no further details on this list have been released by the government.
\item Gonzales & Hayden Press Briefing, supra note 36. Although the 48-point checklist is referenced in this and other articles, the actual list has not been released or explained by the Bush Administration or the intelligence community. To date, no further details on this list have been released by the government.
\end{enumerate}
\end{footnotesize}
United States or a member of a terrorist organization. If the anonymous intelligence officials are credible, the 48-point checklist provides a basis for evaluating the Terrorist Surveillance Program in the context of FISA requirements.

The officials, interviewed in the article said the first step in the checklist is to determine if the target is based in the United States or is communicating with someone in the United States and U.S. or allied intelligence or law enforcement indicates the target is engaged in terrorism or terrorism related activities. This would include the PATRIOT Act’s modified definition of domestic terrorism, which includes attempting to coerce or intimidate U.S. citizens.

The 48-point checklist has not been released, so it is difficult to determine what constitutes a “reasonable basis” for suspicion of terrorist activities; however, the second step in the checklist, gives “one of three” NSA officials power to authorize a wiretap. It is not clear from the intelligence officials accounts whether this authorization for wiretap would be finalized with an official warrant from a Foreign Intelligence Surveillance Court judge.

The next step requires that “technicians” work with telecommunications company executives to intercept the communications. Whether that technician will be a government or corporate employee was not explained by the anonymous intelligence sources.

Finally, the intelligence officials said the NSA notified the appropriate law enforcement agency when terrorism is suspected, but does not necessarily disclose the source of its

\[61\text{ Id.}\]

\[62\text{ Id.}\]

\[63\text{ Section 802 of the PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, amends the U.S. Code, 18 U.S.C. 2331, defining “domestic terrorism” as activities that (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended--(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and (C) occur primarily within the territorial jurisdiction of the United States.}\]

\[64\text{ Gonzales & Hayden Press Briefing, supra note 36.}\]
information. This step capitalizes on the PATRIOT Act’s amendment to FISA that foreign intelligence be only a “significant purpose” in intelligence gathering under the statute. In this process, information that is of a criminal nature may be shared with law enforcement, but the primary purpose of the surveillance is still foreign intelligence in the War on Terror.

The anonymous intelligence officials said that the “identity of the party is suppressed” and the “content of the communication is destroyed” if the intelligence does not ultimately reveal a terrorist connection. This step would make it difficult for any court to determine the legality of the surveillance methods used to monitor suspected terrorists. When evidence of unsubstantiated surveillance is destroyed, there is no evidence to use in monitoring the constitutionality of the NSA’s actions.

Attorney General Alberto Gonzales sent a letter to the Senate Judiciary Committee on January 17, 2007, informing Congress that a judge for the Foreign Intelligence Surveillance Court authorized the Government to collect international communications when one party to the correspondence was believed to be associated with a terrorist organization. This order brought the activities of the TSP under the judicial oversight of the FISA Court. Gonzales, in the letter, said that he believed the Terrorist Surveillance Program always complied with the law. It is unclear whether the FISA court had provided individual warrants or whether it had issued

65 Id.
66 Id.
68 Id.
blanket approval for NSA surveillance activities. Gonzales said the administration would not reauthorize the program when it expired.

Contemporary Cases

Until recently, the First Amendment implications of advances in the technological, regulatory and statutory terms of surveillance have not received significant legal attention in the courts. However, dozens of lawsuits, in response to Bush’s public disclosure of the Terrorist Surveillance Program, are currently pending in the courts. Three cases have been selected for review based on their status as the few post-September 11th suits—involving plaintiff who sued the government for violating their First Amendment rights—which have received significant judicial advancement and media attention.

In Hepting v. AT&T (hereinafter Hepting), the plaintiffs’ claim telecommunication companies partnered with the government in its surveillance programs, violating free expression and privacy. In Center for Constitutional Rights v. President George W. Bush (hereinafter CCR), the defendants claim the Terrorist Surveillance Program violated their rights to free expression under the First Amendment, and their rights to privacy under the Fourth Amendment. A multi-jurisdiction review board has recently consolidated the CCR and Hepting cases. Currently, the Hepting and CCR cases are pending in the Ninth Circuit.

In American Civil Liberties Union v. National Security Agency (hereinafter ACLU), the Terrorist Surveillance Program was found to be a violation of citizens’ First Amendment rights to free speech, in that it chilled their phone communications—an important tool for political discussion. In the decision, the only one so far in the crop of cases filed in response to the

---


70 Gonzales letter, supra note 67.
Terrorist Surveillance Program, United States District Court for the Eastern District of Michigan Judge Anna Diggs Taylor acknowledged the First amendment implications, but she did not extensively address the issue. Instead, she based her decision on the legality of the Terrorist Surveillance Program against the Fourth Amendment’s protection of individual privacy. The Sixth Circuit Court of Appeals struck down the ACLU decision. The plaintiffs appealed the case to the U.S. Supreme Court, who declined the case.

Hepting v. AT&T

In response to the Terrorist Surveillance Program, Tash Hepting, Gregory Hicks, Carolyn Jewel and Erik Knuzen filed a class action lawsuit in January of 2006 alleging that the AT&T Corporation acts as an agent of the government in intercepting private phone communications without a warrant. The Hepting case raised a new issue in electronic surveillance that had not yet been addressed by the judiciary—the partnership between telecommunication companies and the government: Are the telecommunications companies acting “under the color of law” when they cooperate with the government’s warrantless electronic surveillance? The Eighth Circuit of the U.S. Court of Appeals defines “under color of law” in its jury instruction manual as acts done “when a person acts or purports to act in the performance of official duties under any state, county or municipal law, ordinance or regulation.”

The Hepting case specifically targets the actions of AT&T, a telecommunications carrier that facilitates millions of daily telephone, Internet and electronic message communications, many of which are stored in company databases. AT&T, the largest telecommunications

---


72 8th Cir. Civil Jury Instr. 4.40 (2001). For an example of application of “under color of law,” see Adickes v. Kress & Co., 398 U.S. 152 (holding that a law enforcement “conspiracy” to deprive a citizen of Fourteenth Amendment due process rights provides the basis for state action).

73 Hepting v. AT&T Corp., No. 3:06-cv-00672-VRW (N.D. Cal. 2006).
provider in the United States, handles hundreds of millions of voice calls daily. AT&T provides long distance services to about 24.6 million residential customers. Additionally, AT&T provides bundled phone and Internet service to about 73 million households in 46 states. As discussed previously in this chapter, technological advancements and congressional legislation promoting competition fueled AT&T’s growth in the telecommunications industry.

The Electronic Frontier Foundation (hereinafter EFF), on behalf of the plaintiffs, claim that AT&T is involved in a government surveillance program that restricts the First Amendment right to express oneself without fear of government retribution. The EFF said that AT&T, in an “illegal collaboration,” opened its facilities and databases to “direct” access and data mining by government agencies, including the NSA. The Electronic Frontier Foundations said that AT&T used “trap and trace” and pen register devices to capture dialing, routing, addressing


75 Id. at para. 24.


78 Id. at paras. 2-8. "Daytona" is a database management technology developed by AT&T laboratories to manage multiple databases including “Hawkeye,” a call detail record for virtually all telephone communications on the domestic network since 2001. A call detail record includes “originating and terminating” telephone numbers, call time and call length. The plaintiffs’ claim states that as of September 2005, the uncompressed data totaled 312 terabytes. “Daytona” also manages “Aurora,” a database that has stored Internet traffic data since 2003. Id. at paras. 47-63.

79 According to 18 U.S.C. § 3127(4), a trap and trace device records originating phone numbers for incoming calls to a specific phone line.
and/or signaling information that was then made available to the government through remote or local access. The EFF also cited a Federal Communications Commission filing from the AT&T merger with the Southwestern Bell Corporation to establish a relationship between AT&T and the government. The filing said that AT&T is a significant provider of telecommunications and information technology to the federal government, including “network services, systems integration and engineering, and software development services to a broad range of government agencies, including those involved in national defense, intelligence, and homeland security.” The FCC filing listed AT&T’s federal customers for telecommunications services, including: the White House, the State Department, the Department of Homeland Security, the Department of Defense, the Department of Justice, and most branches of the armed forces. In the FCC filing AT&T said it was involved in classified contracts that required it to employ people with government security clearance. AT&T, in the FCC filing, said the company supported the national security infrastructure through its participation in all of the “key fora” for supporting U.S. Government “national security objectives.”

The Hepting plaintiffs’ make six counts against AT&T. Only five counts will be examined for the purpose of this research since the sixth count falls beyond the federal scope of this paper. Each count will be outlined and examined individually. The plaintiffs are seeking an

80 According to 18 U.S.C. § 3127(3), a pen register records all numbers dialed out from a specific phone line.


83 Id. In count six, the plaintiffs claim AT&T engages in unlawful and deceptive business practices in violation of California Constitution Article I §I Business and Professional Code §17200 et. Seq. In addition to the complaints regarding deceptive and unlawful business practices, the plaintiffs claim that AT&T installed pen registers and trap and trace devices without obtaining a court order.
injunction against the defendant’s participation in the program, as well as statutory and punitive damages.\footnote{Amended complaint for damages, declaratory and injunctive relief, Hepting v. AT&T Corp., No. C-06-0672-JCS (N.D. Cal. filed Feb. 22, 2006), available at \url{http://www.eff.org/files/filenode/att/att_complaint_amended.pdf}.}

**Count one**

The plaintiffs said AT&T acts as an agent of the government in violating the First and Fourth Amendment rights of the plaintiffs represented by the Electronic Frontier Foundation. The plaintiffs, including Tash Hepting, Gregory Hicks, Carolyn Jewel and Erik Knuzen, said the Fourth Amendment guarantees them a “reasonable expectation of privacy in their communications stored by AT&T.”\footnote{\textit{Id.} at paras. 78-80.} This reasonable expectation of privacy encompasses the right to speak or receive speech anonymously and to associate privately.\footnote{\textit{Id.}} The plaintiffs in the \textit{Hepting} case said that their private communications were intercepted, disclosed and divulged at the direction of the government. The plaintiffs said that AT&T continues to act as an agent of the government “with deliberate indifference” or “reckless disregard” for plaintiff’s First, Fourth and Fourteenth amendment rights through its disclosure of customer information.

The plaintiffs complained AT&T acts in the interest of government investigators and not in the interest of protecting “its own property or rights,” including customer communications and company networks. The plaintiff’s claim did not emphasize the application of the constitutional amendments, as much as it looks at the industry-government relationship in light of AT&T’s privacy policy.\footnote{AT&T has a privacy policy, which sets clear guidelines under which it will protect or release private customer information.}
Title 18 of the U.S. Code provides legal immunity for a telecommunications company that provides government database access, as long as the government produces documentation of security concerns as justification for the surveillance.\(^8\) AT&T’s Privacy Policy says it will not disclose customer information without customer consent or a “subpoena, search warrant, or other legal process.” The privacy policy also allows for disclosure in the “case of imminent physical harm to the customer or others.”\(^9\) The documentation for the subpoena or search warrant does not have to be a traditional court order; but it must be a written formal request from the Attorney General, whether or not there is a court order.\(^10\) If AT&T can prove there was a formal request, then it will negate the issue of whether providing the NSA access to databases runs counter to the constitution’s protection of negative liberty. If the Attorney General issued a formal request for cooperation, AT&T is not liable as an agent of the government. AT&T would be working within the framework of the law and not therefore, in collusion with the government under color of law.

**Count two:**

The plaintiffs also alleged that AT&T acquires communications through electronic surveillance without consent of at least one party engaged in the communication, as required by AT&T’s privacy policy. The plaintiffs said AT&T acts as an agent of the government by engaging in this electronic surveillance “under color of law.” Electronic surveillance under color of law, and not authorized by statute, is criminalized by 50 U.S.C. § 1809.\(^9\) Electronic surveillance is defined as the electronic, mechanical or other interception of communications

---

\(^8\) Title 18 Part I Chapter 119 §2511(2)(a)(ii)(A)(B).


sent or received by a person who is in the United States. The interception, whether or not intentional, requires the consent of at least one of the parties involved or a warrant for law enforcement purposes. The plaintiffs said that AT&T engaged in electronic surveillance and intentionally disclosed the acquired information without statutory authorization. Plaintiffs said they were never given a chance to consent to the surveillance; nor was the surveillance disclosed to them after the fact. Plaintiffs also alleged that there is a strong likelihood the surveillance is ongoing. If AT&T engaged in electronic surveillance without consent of at least one party, and with statutory authorization, then it could be seen as an agent of the government in violation of U.S. laws.

The Bush Administration defended the Terrorist Surveillance Program by saying the Authorization for the Use of Military Force adopted by Congress shortly after the September 11th attacks permitted the executive branch to order warrantless surveillance. If an official document exists ordering AT&T to participate in the Terrorist Surveillance Program, then the surveillance could be seen as legal since AT&T’s privacy policy allows disclosure of customer information when authorized by official government order. Disclosure is also legal under 50


93 Id. See Amended complaint for damages, declaratory and injunctive relief at para. 93, Hepting v. AT&T Corp., No. C-06-0672-JCS (N.D. Cal. filed Feb. 22, 2006), available at http://www.eff.org/files/filenode/att/att_complaint_amended.pdf. According to the FBI, under "color of any law" includes "acts not only done by federal, state, or local officials within the bounds or limits of their lawful authority, but also acts done without and beyond the bounds of their lawful authority; provided that, in order for unlawful acts of any official to be done under "color of any law," the unlawful acts must be done while such official is purporting or pretending to act in the performance of his/her official duties. This definition includes, in addition to law enforcement officials, individuals such as Mayors, Council persons, Judges, Nursing Home Proprietors, Security Guards, etc., persons who are bound by laws, statutes ordinances, or customs.” See http://www.fbi.gov/hq/cId./civilrights/statutes.htm#anchor25114.


95 Id.

U.S. 1809(b) when the government produces a court order or warrant authorizing the surveillance.\textsuperscript{97} AT&T’S privacy policy also allows disclosure of customer information when authorized by a court order, even when neither of the parties engaged in the communication are notified.

The policy says

AT&T will not sell, trade, or disclose to third parties any customer identifiable information derived from use of an AT&T online service without customer consent or official court order.\textsuperscript{98}

Additionally, the AT&T privacy agreement says AT&T may also use customer identifiable information to investigate and help prevent potentially unlawful activity or activity that threatens the network or otherwise violates the customer agreement for that service."\textsuperscript{99} The customer agrees to the terms of the privacy policy through notification and continued use of services.\textsuperscript{100}

\textbf{Count three}

The plaintiffs allege the plaintiff intercepts customer communications in violation of 18 U.S.C.§2511, the section of the U.S. code that governs crimes and criminal procedures in relation to the interception and disclosure of wire, oral or electronic communications. This is different from count one, which makes a claim against the constitutionality of the surveillance. It is also different from count two, which makes a claim against the legality of AT&T’s involvement under the chapter of the U.S. code which governs War and National Defense.

“Interception”, an “attempt to intercept” or “arrangement to intercept” any wire, oral or

\textsuperscript{97} 50 U.S.C 1809(b).

\textsuperscript{98} AT&T Privacy Policy, \url{http://www.att.com/privacy/} (last visited June 22, 2008).

\textsuperscript{99} Id.

\textsuperscript{100} Id.
electronic communication is prohibited by 18 U.S.C. §2511. Disclosure or transmission of contents obtained or generated through surveillance is also prohibited. The plaintiffs says that AT&T “intentionally intercepted, endeavored to intercept, or procured another person to intercept or endeavor to intercept” electronic communications. They claim the information was intentionally disclosed to government intelligence agents.

This count can be evaluated in a manner similar to the evaluation of count two. Title 50, discussed in count two, is the War and National Defense Chapter of the U.S. Code. Title 18, in contrast, deals specifically with wiretapping from a criminal perspective. Title 18 deals specifically with the relationship between the government and a telecommunications provider collaborating for the purpose of electronic surveillance. Employees of telecommunication providers are forbidden from engaging in “random monitoring” of communication service, except in the case of quality control checks. However, Title 18 “authorizes” employees to provide information, facilities and technical assistance to intelligence officials that provide a court order or written certification by the Attorney General.

When a statute, court order or written authorization sanctions provider cooperation, there is no cause of action against the provider. As in Count Two, if AT&T can establish they were acting under an official government order, they will not be liable under Title 18. AT&T would


102 Id.


104 Id. at para. 103/


107 Id.
also be exempt from prosecution under this count if the Authorization for Use of Military Force were seen as a statutory basis for the Terrorist Surveillance Program. The provider and its representatives are also prohibited from disclosing the “existence of any interception or surveillance or the device used to accomplish the interception or surveillance” when a court order is executed. When the company is acting to comply with this section, it cannot be the subject of court action.

**Count four**

The plaintiffs claimed AT&T divulges or publishes the “existence, contents, substance, purport, effect or meaning “of the plaintiffs’ communications in violation of 47 U.S.C§605(a), the section of the United States code which establishes federal telecommunication regulations. Title 47 prohibits “divulging or publishing” electronically stored communications unless authorized by court order or another lawful authority. If a letter from the Attorney General was issued to AT&T, then that written authorization should satisfy this legal requirement and nullify this count in the case.

**Count five**

Plaintiffs allege that AT&T illegally divulged electronic communication records to a governmental entity in violation of 18 U.S.C.§2702, which prohibits the disclosure of electronic subscriber records to anyone except as needed for internal customer service. This count is similar to the plaintiffs’ claim in count four that the AT&T divulged customer communications;

---


109 Amended complaint for damages, declaratory and injunctive relief at paras. 112-113, Hepting v. AT&T Corp., No. C-06-0672-JCS (N.D. Cal. filed Feb. 22, 2006), available at http://www.eff.org/files/filenode/att/att_complaint_amended.pdf. Disclosure can legally take place in certain cases, such as disclosure to officers of communication centers, masters of ships, attorneys or the addressee of the intercepted communication.

the key difference between the two counts is that in this count, the plaintiff’s make the claim that AT&T provided the government with subscriber records for a purpose other than internal customer service. If it can be established that AT&T disclosed customer identifiable information to the government, the plaintiffs could have grounds under this count. However, based on the privacy policy that consumers agree to in using the service, discussed in count two, the disclosure of the records would technically be made with the consent of the customer. The customer, in using provider services, agrees to the privacy policy which allows for disclosure authorized by warrant, court order, or cause to believe the customer intends to “harm” themselves or someone else. AT&T is accused of participating in the “Terrorist Surveillance Program,” but terrorist by nature seek to harm others.

**Hepting v. AT&T: First Amendment issues**

The complaint filed by the EFF challenges the legality of AT&T’s participation in the Terrorist Surveillance Program and asks that the action be seen as a violation of the plaintiff’s First Amendment rights under the U.S. Constitution. The complaint states that the plaintiff’s First Amendment rights to speak and receive speech anonymously and associate privately are violated by the program. The EFF suggests that the actions of the defendants AT&T and telephone companies involved in the TSP represent “a credible threat of immediate future harm.” Only one of the individual plaintiffs, Carolyn Jewel, explained the actual harm she suffered. Gregory Hicks and Erik Knutzen only described their communication activities.

---


112 Id. at para. 85.

113 Id. at para. 88.
• Gregory Hicks, a retired Naval Officer and systems engineer, has been a San Jose, California subscriber of AT&T Corporation’s residential long distance telephone service since February 1995. He regularly used the service to call Korea, Japan and Spain.\textsuperscript{114}

• Carolyn Jewel, a database administrator and author, has been a Petaluma, California subscriber of AT&T Corporation’s Worldnet service since June 2000. She used the service to send and receive e-mail with correspondents in England, Germany and Indonesia.\textsuperscript{115} In her statement for the court, Jewel said that she has been concerned about the privacy of her communications since learning about the TSP. As an example, she cited her limited responses to an Indonesian Muslim acquaintance’s inquiries into her understanding of Balinese Islamic practice. She also has avoided discussing U.S. action in Iraq with him. She says she would have limited her communications even sooner had she known of the TSP.\textsuperscript{116}

• Erik Knutzen, a photographer and land use researcher was a Los Angeles, California subscriber of AT&T Corporation’s Worldnet from October 2003 to May 2005. He used the service to send and receive both domestic and international e-mail.\textsuperscript{117}

\textbf{Hepting v. AT&T: state secrets}

The Hepting case has raised another issue, beyond the constitutional protections afforded to private phone communications. The case has yet to be decided and this is due in part to the sensitive nature of the information that the plaintiffs are seeking to introduce as evidence in establishing their claims.

Mark Klein worked as a technician for AT&T for over 20 years.\textsuperscript{118} Klein filed a declaration with the court that was released in a redacted version on June 8, 2006. He had

\textsuperscript{114} Id., at para. 14.

\textsuperscript{115} Id., at para. 15.


previously issued a public statement on April 6, 2006.\textsuperscript{119} Klein’s public statement contains more details than the heavily redacted version filed with the court, although they offer the same version of his employment activities. Klein said that in 2002, while he was working at an AT&T office in San Francisco, he met an NSA agent who was interviewing a technician for a job.\textsuperscript{120} He said that in 2003, he saw a room being built in the AT&T Folsom Street headquarters in San Francisco.\textsuperscript{121} Klein said that the NSA agent that was interviewed was eventually hired to staff the new room where public calls would be routed.\textsuperscript{122}

Klein said he learned, in the course of his job duties, that fiber optic cables from the secret room were tapping into the WorldNet circuits, “splitting off a portion of the light signal.”\textsuperscript{123} Klein also described documents, which listed equipment in the secret room including the Narus STA 6400, a semantic traffic analyzer that can sift through Internet data looking for “preprogrammed targets.”\textsuperscript{124} Klein said he knew of other splitters being installed in cities including Seattle, San Jose, Los Angeles and San Diego.\textsuperscript{125} Klein described the NSA monitoring capabilities as a “vacuum-cleaner surveillance” of all data crossing the Internet.\textsuperscript{126}

\begin{scriptsize}
\begin{itemize}
\item[{\textsuperscript{121}}] \textit{Id.}
\item[{\textsuperscript{122}}] \textit{Id.}
\item[{\textsuperscript{123}}] \textit{Id.}
\item[{\textsuperscript{124}}] \textit{Id.}
\item[{\textsuperscript{125}}] \textit{Id.}
\item[{\textsuperscript{126}}] \textit{Id.}
\end{itemize}
\end{scriptsize}
On April 28, 2006, three weeks after the media released Klein’s statement, the U.S. government filed a statement of interest in the *Hepting* case. The statement said the government would provide an assertion of the state secrets privilege, a motion to intervene and a motion to dismiss the case by May 12, 2006.\(^{127}\) The government asked the court to suspend discovery until the motions were filed.\(^{128}\) The plaintiffs submitted several documents to the court under seal at the request of the Department of Justice. The DOJ is not a plaintiff in the case, but it said unsealing the documents might compromise national security. The plaintiffs said the exclusion of these documents could result in the dismissal of the case.\(^{129}\)

Department of Justice said the parties in the case (both plaintiffs and AT&T executives) are not sufficiently informed to speak on the sensitivity of the documents sealed in this case.\(^{130}\) The government said there is judicial precedent for government intervention in cases between private parties when “sensitive military secrets” are the central focus of litigation.\(^{131}\) In its statement of interest, the government also cited the 1998 decision of the U.S. Court of Appeals in *Kasza v. Browner*, upholding the use of the state secrets privilege to exclude information from a


\(^{129}\) United States v. Reynolds, 345 U.S. 1 (1953) at 11 n.26 (holding that the government can claim the state secrets privilege in cases involving national security if it can show reasonable cause for privilege)


\(^{131}\) *Fitzgerald v. Penthouse Int’l, Ltd.*, 776 F.2d 1236, 1239, 1241-42 (4th Cir. 1985) (holding that a case can be dismissed if a trial would lead to disclosure of state secrets).
case where plaintiffs alleged the Air Force had improperly handled toxic waste in a classified operating area.132

On May 13, 2006, John Negroponte, the director of National Intelligence, filed a declaration invoking the military and state secrets privilege under the National Security Act.133 Negroponte’s statement says that disclosure of evidence contained in the testimony of Mark Klein would cause “exceptionally grave damage” to U.S. national security.134 Negroponte also said the Terrorist Surveillance Program, as authorized by the President, gave the NSA the legal authority to collect “certain one-end foreign communications.” He did not elaborate on this description, saying that further details of the program would disclose classified intelligence information. Keith B. Alexander, the director of the National Security Agency, also filed a declaration on May 13, supporting Negroponte’s assertion of state secrets privilege.135

---

132 Kasza v. Browner, 133 F.3d 1159 (9th Cir. 1998). (The court also said that submission of classified material for in camera, ex parte review is “unexceptional” in cases where the state secrets privilege is invoked; therefore sensitive information should be separated from nonsensitive information to allow for disclosure of nonsensitive information).


The Director of National Intelligence (DNI) serves as the head of the Intelligence Community (IC), overseeing and directing the implementation of the National Intelligence Program and acting as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the national security. Working together with the Principal Deputy DNI (PDDNI) and with the assistance of Mission Managers and four Deputy Directors, the Office of the DNI's goal is to effectively integrate foreign, military and domestic intelligence in defense of the homeland and of United States interests abroad.


Alexander asked the judge to dismiss the case in the interest of preventing “harms” to U.S. national security that would occur if it were litigated.136

**Hepting v. AT&T: developments**

A major obstacle for the plaintiffs in a case of this nature is establishing AT&T’s involvement in the Terrorist Surveillance Program.137 The December 2005 *New York Times* article reported cooperation between telecommunications corporations and the government, but did not specifically name companies that had participated in the Terrorist Surveillance Program. A survey of telecommunication providers conducted by CNET, an Internet publisher of computer and technology news and information, attempted to discover which of the major telecommunications companies might be involved.138 CNET, in early February of 2006, asked national telecommunication providers if they had participated in the Terrorist Surveillance Program.139 Of the companies polled, fifteen said they had not been part of the program. Twelve companies chose not to reply, some citing “national security” as the reason. AT&T spokesman Dave Pacholczyk said, “We don’t comment on matters of national security.”

According to a February 2006 report by *USA Today*, seven telecommunications executives anonymously admitted that the government had eavesdropped on international calls by suspected terrorists without warrants.140 AT&T, MCI and Sprint publicly denied participation in the

---

136 Id.

137 JAMES RISEN, *STATE OF WAR: THE SECRET HISTORY OF THE C.I.A. AND THE BUSH ADMINISTRATION* (2006). Like the WWII companies who were party to secret government surveillance, information about company involvement in the program is almost certainly limited to upper level executives.


139 Declan McCullagh & Anne Broache, *Some companies helped the NSA, but which?* CNET News.com, Feb. 6, 2006 (last visited June 14, 2008).

program, but anonymous executives levied claims of the companies’ involvement.\textsuperscript{141} Publicly, companies such as AT&T are offering a no comment to the media, perhaps due to national security reasons cited by Negroponte in his declaration in the Hepting case. Anonymously, executives say industry and government are partnered in the surveillance. It is possible that the executives are forbidden by court order from officially revealing assistance provided to the government in the Terrorist Surveillance program.\textsuperscript{142}

Even if AT&T is not bound by a court order preventing discussion of the program, it is unlikely this case would be successful based on court reactions to past claims naming corporations as parties to the government’s warrantless surveillance. In the 1982 case of Halkin \textit{v. Helms}, the United States Court of Appeals for the District of Columbia Circuit held that courts must defer to executive expertise when assessing executive privilege in handling information that poses a reasonable danger to secrets of state.\textsuperscript{143} In the \textit{Halkin} case, Adele Halkin filed a lawsuit on behalf of herself and twenty-seven other Vietnam War activists and organizations that claimed the government had intercepted their “international wire, cable and telephone communications” without a warrant.\textsuperscript{144} The plaintiffs demanded the release of the government-held information about their own communications. The \textit{Halkin} case is a relevant precedent in \textit{Hepting} because—in addition to the NSA, CIA, FBI, Secret Service and Defense Intelligence Agency—the three communications giants who cooperated with the government’s Operation Shamrock during WWII were also listed in the \textit{Halkin} case as defendants.\textsuperscript{145}

\begin{thebibliography}{99}
\bibitem{Id.} Id.
\bibitem{Title 18§2511(2)(a)(ii)(B).} Title 18§2511(2)(a)(ii)(B).
\bibitem{Halkin v. Helms, 598 F.2d 1, 83 (D.C. Cir. 1978).} Halkin \textit{v. Helms}, 598 F.2d 1, 83 (D.C. Cir. 1978).
\bibitem{Id.} Id.
\bibitem{Id.} Id.
\end{thebibliography}
International, RCA Global Communications, and ITT World Communications were named in the *Halkin* case, which was filed in response to a situation remarkably similar to what the *Hepting* plaintiffs’ allegations.

The *Halkin* case did not directly consider the role of the telecommunication corporations in the illegal surveillance. Instead, the court found for the defendants based on state secret privilege, that is, the government could invoke state-secrets privilege if the divulgence of a discovery material would compromise national security.\textsuperscript{146} The court says that the “state secrets privilege is absolute.”\textsuperscript{147} The court added that, “The superiority of well-informed advocacy becomes less justifiable in view of the substantial risk of unauthorized disclosure of privileged information.”\textsuperscript{148} Without evidence demonstrating that the plaintiffs were actually the subjects of illegal surveillance, the *Hepting* case would have no basis.

On May 17, 2006, Judge Vaughn R. Walker of the U.S. District Court for the Northern District of California denied AT&T’s motion to compel the return of documents attached to the testimony of Mark Klein.\textsuperscript{149} Judge Walker ordered the documents to be kept secure by the EFF, as they were still sealed under court order. On June 6, 2006 Judge Walker issued an order stating that the case “cannot proceed” until the court examined the classified documents to decide to “what extent” the state secrets privilege might apply.\textsuperscript{150} In the order, Judge Walker ordered the

\textsuperscript{146} *Id.*

\textsuperscript{147} *Id.* at 88.

\textsuperscript{148} *Id.*


\textsuperscript{150} *Id.*
government to provide the classified documents for in camera review no later than June 9.\textsuperscript{151}

Subsequently, oral arguments were heard on June 23, 2006.\textsuperscript{152}

On July 20, 2006, the court issued an order denying the government’s motion to dismiss the case.\textsuperscript{153} The court said that deferring to a “blanket assertion of secrecy” would abdicate the judicial responsibility to the United States Constitution.\textsuperscript{154} Furthermore, the court said that dismissing the case would “sacrifice liberty for no apparent enhancement of security.”\textsuperscript{155} On July 20, the court denied the government’s motion to dismiss the case.\textsuperscript{156} The court order stated that the state secrets privilege had limits.\textsuperscript{157} The court said that deferring to a “blanket assertion of secrecy” would abdicate the judicial responsibility to the United States Constitution.\textsuperscript{158}

\textsuperscript{151} Id. at p. 7, lines 11-17.


\textsuperscript{157} Id.

\textsuperscript{158} Id.
Furthermore, the court said that dismissing the case would “sacrifice liberty for no apparent
enhancement of security.”\textsuperscript{159} The court said that based on publicly available information, details
of government monitoring of communication content would not reveal any new information to
terrorists.\textsuperscript{160} The court also ruled on the public disclosure of information regarding
“communication content” versus the monitoring of “communication records,” stating that the
latter’s existence is unclear.\textsuperscript{161} On August 2, the court issued a stay of proceedings pending
appeal.\textsuperscript{162}

On August 9, 2006, over a dozen cases were consolidated before Judge Walker from suits
against the government and telecommunications companies with plaintiffs alleging illegal
surveillance under the Terrorist Surveillance Program.\textsuperscript{163} The Judicial Panel on Multidistrict
Litigation found that seventeen cases involved “common questions of fact,” and should therefore
be centralized in the Northern District of California to “serve the convenience of the parties and
witnesses and promote the just and efficient conduct” of the legislation of the cases. All of the
class action suits that were consolidated involved “alleged Government surveillance by

\begin{itemize}
  \item \textsuperscript{159} Id.
  \item \textsuperscript{160} Id.
  \item \textsuperscript{161} Id.
  \item Order granting motion to stay until Aug. 8 (Doc. No. 330), Hepting v. AT&T Corp., No. 3:06-cv-00672-VRW
  \item In re Nat’l Sec. Agency Telecommunications Records Litigation, 444 F. Supp. 2d 1332 (JPML Aug 9, 2006)
    (No. MDL-1791). The consolidated cases include: Conner v. AT&T Corp., No. 1:06-632 (E.D. Cal. 2006); Souder
    v. AT&T Corp., No. 3:06-1058 (S.D. Cal. 2006); Schwarz v. AT&T Corp., No. 1:06-2680 (N. D. Cal. 2006); Terkel
    2006); Fuller v. Verizon Commc’ns, Inc., No 9:06-77 (D. Mont. 2006); Dolberg v. AT&T Corp., No. 9:06-78 (D.
    Mont. 2006); Marck v. Verizon Commc’ns, Inc., No. 2:06-2455 (E.D.N.Y. 2006); Mayer v. Verizon Commc’ns,
    Inc., No. 1:06-3650 (S.D.N.Y. 2006); Hines v. Verizon Nw., Inc., No. 3:06-694 (D. Or. 2006); Bissit v. Verizon
    Commc’ns, Inc., No. 1:06-220 (D.R.I. 2006); Mahoney v. AT&T Commc’ns, Inc., No. 1:06-223 (D.R.I. 2006); Mahoney
    v. Verizon Commc’ns, Inc., No. 1:06-224 (D.R.I. 2006); Potter v. BellSouth Corp., No. 3:06-469 (M.D.
    Tenn. 2006); Trevino v. AT&T Corp., No. 2:06-209 (S.D. Tex. 2006); Harrington v. AT&T Inc., No. 1:06-374
    (W.D. Tex. 2006).
\end{itemize}
individual telecommunications companies.” The consolidation was made for three reasons given by the court: 1) to eliminate duplicate discovery, prevent inconsistent pretrial rulings and conserve resources; 2) to place all cases under the jurisdiction of the California court where the “more advanced” *Hepting* action was taking place; and 3) to address the Government’s security concerns over “production of highly classified information.”

On August 14, 2006, the court granted AT&T another stay of proceedings pending appeal. On November 7, 2006, the U.S. Court of Appeals for the Ninth Circuit granted AT&T’s request for an appeal.

On February 15, 2007, six additional cases were consolidated with the Hepting suit. The United States Judicial panel for the Ninth Circuit notified the parties in the consolidated cases, which include: *United States v. Rabner, United States v. Gaw, Clayton/Gaw v. AT&T, United States v. Adams, United States v. Palermino, and United States v. Volz.* The cases were transferred to the Northern District of California for “coordinated pretrial proceedings” with the Hepting case. In part, the transfer was made due to the fact that the “United States challenges the authority of state officials to seek information from telecommunications carriers about alleged foreign intelligence activities of the United States on the grounds, inter alia, that such state demands are precluded by the Constitution and preempted by federal law”:

---


167 *Id.* The cases are United States v. Rabner, No. 06-cv-2683 (D.N.J. 2006); United States v. Gaw, No. 06-1-cv-1132 (E.D. Mo. 2006); Clayton/Gaw v. AT&T, No. 06-cv-4177 (W.D. Mo. 2006); United States v. Adams, No. 06-cv-0097 (D. Me. 2006); United States v. Palermino, No. 06-cv-1405 (D. Ct. 2006); United States v. Volz, No. 06-cv-188 (D. Vt. 2006).
These six actions involve common questions of fact with the actions in this litigation previously centralized in the Northern District of California, and that transfer of the six actions to the Northern District of California for inclusion in the coordinated or consolidated pretrial proceedings in that district will serve the convenience of the parties and witnesses.168

On February 20, 2007, U.S. District Court Judge Vaughn Walker opened the discovery process in the case, denying the government and AT&T’s request to freeze proceedings while the Ninth Circuit of the U.S. Court of Appeals decided the question of state secrets privilege. Walker also denied the request for a blanket stay for the other telecommunications surveillance cases transferred to his court.169 Additionally, Walker certified the case for appeal.

On August 15, 2007, the Ninth Circuit Court of Appeals heard arguments in the consolidated civil lawsuit, including Hepting.170 Judges Harry Pregorson, Michael Daly Hawkins and M. Margaret McKeown presided over arguments from attorneys representing the United States government, AT&T and the Electronic Frontier Foundation.171 The appeal hearing took place in San Francisco and the court looked at two issues related to the surveillance program: 1) do the plaintiffs have standing to sue based on actual injury by the government program; and 2) do national security concerns justify dismissal of the case under state secrets privilege?172


172 Id.
U.S. Deputy Solicitor General Gregory Garr argued on behalf of the government, telling the court what the federal government contended was the court’s role in the proceedings:

Your job is to determine whether or not the requirements of the [secrets] privilege have been properly met. And that includes the declaration, the sworn declaration of the head of the agency asserting the privilege, and the assertion that that individual asserting it has personal knowledge of the matter [at hand]. 173

Garr also argued that the review of any documents establishing the state secrets privilege would jeopardize national security. 174 He, along with AT&T attorney Mike Kellogg, also questioned the validity of the evidence filed on behalf of former AT&T technician Mark Klein. Garr said, of the evidence:

The plaintiffs in this case allege that there is a secret room at AT&T and that alleged activities are taking place in that room. They have no proof of that except the affidavit from someone who says that there’s a leaky air-conditioner and some poorly installed cable in the room, which is hardly consistent with this sort of breathtaking program they have in mind. 175

Kellogg said that AT&T was legally prohibited from disclosing any information that would jeopardize national security:

I’d like to make three points today focused on the issue of plaintiffs’ standing. And the first point is that the questions that the Court would have to resolve in order to determine that the plaintiffs have standing are the very questions as to which the government has invoked the state-secrets privilege. In other words, they would have to show not only that there is such a dragnet program but that AT&T participated in it and that their own individual communications were captured pursuant to that. But those precise questions which are necessary to standing are ones that the government, invoking the state-secrets privilege according to proper procedures, have said cannot be litigated and cannot be resolved one way or another. AT&T is not allowed to put in any defense with respect to those questions. Evidence is not allowed to be presented on those questions. Under those circumstances, at this stage in the litigation, as you asked, Judge McKeown, courts have

173 Id. at 6.
174 Id.
175 Id.
repeated said that once it becomes clear that the very questions at issue cannot be litigated, the case has to be dismissed.\textsuperscript{176}

Judge Pregerson asked Garr whether a warrant was obtained in this case, specifically, if the government went through the FISA court in the case.\textsuperscript{177} Garr responded that the answer to that question was “protected by the state secrets.”\textsuperscript{178} When Judge McKeown pressed for an answer, Garr said he could not say whether or not the FISA court held proceedings on the case because, “it would disclose methods or means or the existence of intelligence.”\textsuperscript{179} Judge Pregerson responded by saying, “everybody knows about the FISA court,” and added

we are getting into the operational details of intelligence capabilities, and the one thing that the intelligence experts will say is the more publicly and the more concretely we educate our adversaries on our intelligence-gathering capabilities, the easier it is for them to evade detection by adapting their means.\textsuperscript{180}

Judge Margaret McKeown addressed the issue of mass surveillance, saying:

Yes, my only question or comment on your final remark is that we have a denial here of broad-spread domestic surveillance. If we didn’t have a denial and if the government were undertaking that, I imagine from your comments that your response would be we can’t—no-one could litigate that kind of an invasion because of the state-secrets doctrine.\textsuperscript{181}

The \textit{Hepting} case is currently pending in the Ninth Circuit.

\textbf{CCR v. Bush}

In \textit{Center for Constitutional Rights, et al. v. George W. Bush, et al.}, filed January 17, 2006, the Center for Constitutional Rights (hereinafter CCR) filed a lawsuit against President George W. Bush on behalf of plaintiffs Tina M. Foster, Gitanjali S. Gutierrez, Seema Ahmad,

\textsuperscript{176} \textit{Id.}
\textsuperscript{177} \textit{Id.}
\textsuperscript{178} \textit{Id.}
\textsuperscript{179} \textit{Id.}
\textsuperscript{180} \textit{Id.}
\textsuperscript{181} \textit{Id.}
Maria Lahood and Rachel Meeropol. 182 The Center for Constitutional Rights is a nonprofit organization that represents people, including Muslim foreign nationals, whose rights have been allegedly violated by intelligence gathering and detention practices since September 11, 2001.183 The plaintiffs claimed they are “within the class of people” described by the government as targets of the TSP.184 The CCR complaint said the Terrorist Surveillance Program created a “chilling effect” on the defendant’s First Amendment right to free speech.185 The plaintiffs claim their conversations with clients and other people “abroad” have been intercepted through the TSP, violating attorney client privilege and inhibiting them from representing their clients “vigorously.”186

The CCR alleged that the government obstructed their “modes” of expression and association under the First Amendment. This includes the ability to 1) provide free legal advice, 2) join together in association for legal advocacy, 3) freely form attorney-client relationships, 4) vigorously advocate for clients, and 5) petition the government for redress of grievances.187

Rachel Meeropool and Maria Lahood made two of the claims of individual harm:

- Rachel Meeropol, an attorney at CCR, said she communicates with witnesses and other people in the Middle East. In her statement, she said that she has become more cautious of what she says in telephone conversations since learning of the Terrorist Surveillance Program.188 She said that since she found out, she has

---

182 Ctr. for Constitutional Rights v. Bush, No. 06-CV-00313. (S.D.N.Y. 2006). The Center for Constitutional Rights, including its lawyers and legal staff, are the plaintiffs in the case.


184 Id. at para. 4.

185 Id. at para. 2.

186 Id., at paras. 5 and 6.

187 Id., at paras. 51 and 52.

reevaluated her communication practices. She felt she couldn’t “safely or ethically” discuss matters with clients via phone.\textsuperscript{189} Meeropol said that having to meet in person delays meetings or forces her to use inefficient postal message delivery.\textsuperscript{190} She concluded her statement by saying that it is “frightening” and “outrageous” that the interception of her attorney-client communications is not subject to judicial oversight.

- Maria Lahood, an attorney for the CCR, said in her statement that she has become “extremely cautious” of her phone conversations with clients since becoming aware of the TSP. She said she is “constantly monitoring” her conversations with a particular client who might be a target of the TSP. Lahood said these conversations are often “deferred” until she can meet with her client in person and that often includes flying out of the country.\textsuperscript{191}

The\textit{ CCR} case was transferred to the San Francisco District Court under Judge Vaughn Walker on December 15, 2006.\textsuperscript{192} On August 9, 2007, attorneys for the CCR asked Judge Walker to find the NSA’s program of warrantless surveillance unconstitutional,” and strike it down based on the chilling effect to the plaintiff’s constitutionally protected activities.”\textsuperscript{193} The Ninth Circuit Court of Appeals will decide the\textit{ CCR} case with\textit{ Hepting}, both of which are pending.

\textbf{ACLU v. NSA}

On January 17, 2006, the same month the Center for Constitutional Rights filed its suit against President Bush, the American Civil Liberties Union filed, in the Eastern United States District Court of Michigan, Southern Division, a complaint for declaratory and injunctive action

\textsuperscript{189} Id. at paras. 4-6.

\textsuperscript{190} Id. at para. 11.

\textsuperscript{191} Id. at paras. 3-5.

\textsuperscript{192} Also transferred were Mink v. AT&T Commc’ns of the Sw., Inc., No. 4:06-cv-01113 (E.D. Mo. 2006) & Shubert v. Bush, No. 1:06-cv-02282 (E.D.N.Y. 2006).

\textsuperscript{193} Plaintiffs’ Supplemental Reply Memorandum, \textit{In re} Nat’l Sec. Agency Telecommunications Records Litigation (N.D. Cal. filed Aug. 9, 2007).
against the National Security Agency. The suit, filed on behalf of journalists, scholars, attorneys and national nonprofit organizations challenged the constitutionality of “a secret government program to intercept vast quantities of the international telephone and Internet communications of innocent Americans without court approval.”194 In the complaint, the plaintiffs said that the Terrorist Surveillance Program violated their Fourth Amendment right to privacy and their First Amendment rights to free speech and association under the U.S. Constitution.195 The plaintiffs complained that the TSP disrupted their ability to “talk with sources, locate witnesses, conduct scholarship, and engage in advocacy.”196

On August 17, 2006, eight months after the ACLU filed suit, Judge Anna Diggs Taylor ruled the Terrorist Surveillance Program to be unconstitutional on First and Fourth Amendment grounds based on the public interest in upholding the constitution.197 Judge Taylor concluded her opinion with a quote from U.S. v. Robel, by Justice Warren in 1967:

Implicit in the term ‘national defense’ is the notion of defending those values and ideas which set this Nation apart. . . . It would indeed be ironic if, in the name of national defense, we would sanction the subversion of . . . those liberties . . . which makes the defense of the Nation worthwhile.198


195 Id. at paras. 3, 192, 193.

196 Id. at para. 2.


198 Id. (quoting United States v. Robel, 389 U.S. 258 (1967) (holding the U.S. government cannot deprive citizens of constitutional protections for free association, even in cases of national security)).
In the decision, Judge Taylor relied upon the reasoning in *Marcus v. Search Warrants*, to highlight the “intellectual matrix within which our own constitutional fabric was shaped.”\(^{199}\) She said the Bill of Rights was created with a historical knowledge of free speech struggles in England. Those struggles were linked to search and seizure. Unrestricted powers of search and seizure can be instruments for “stifling liberty of expression.”\(^{200}\) As precedent, Judge Taylor relied on the reasoning of the court in the 1965 *Dombrowski v. Pfister* case, where the Supreme Court struck down a Louisiana statute mandating that members of communist organizations register with the government. In *Dombrowski*, the Court held that intrusive government surveillance could create a chilling effect on free expression.\(^{201}\)

In *ACLU v. NSA*, Judge Taylor said that FISA prohibits surveillance based solely on First Amendment protected activities like free expression.\(^{202}\) She then said national security cases were of a “special nature” because they involve a convergence of First and Fourth Amendment values. She said this convergence posed a greater risk to constitutionally protected speech.\(^{203}\) She ruled that President Bush, in authorizing the TSP, violated the Constitution in failing to provide Fourth Amendment privacy protection for First Amendment protected speech that

---

\(^{199}\) *Id.* (citing *Marcus v. Search Warrants*, 367 U.S. 717 (1961) (holding that states, under the Fourteenth Amendment’s due process clause, cannot seize obscene publications because the materials removal from the market amounts to a violation of the First Amendment’s protection for free speech and press)).

\(^{200}\) *Id.* (quoting *Marcus*, 367 U.S. 717 at 729).


challenged administrative policies through unorthodox political beliefs. Bush’s authorization of the TSP was an intrusive government action, which chilled the defendant’s right to free expression.

The defendants in the case had relied on the 1971 case of Laird v. Tatum to argue a “chilling effect” of First Amendment rights based on “speculative fears” of the TSP. In Laird, the plaintiffs had claimed that the existence of an Army domestic surveillance program of civil disturbances chilled their associational rights. Judge Taylor distinguished the ACLU issue from Laird because, she said, plaintiffs were not arguing a chilling effect based on the notion that they “could conceivably” become subject to surveillance under the TSP, but that continuation of the TSP has chilled their activities such as making international and national calls, and carrying out professional responsibilities. Taylor said the distinction was that the TSP actually chilled the defendants First Amendment expressions, whereas in Laird, the chilling effect was purely speculative.

Plaintiffs would be able to continue using the telephone and email in the execution of their professional responsibilities if the Defendants were not undisputedly and admittedly conducting warrantless wiretaps of conversations.

Examples of the types of concrete injuries alleged in the case can be found in the original complaint filed by the plaintiffs who believe their communications are being intercepted illegally under the TSP. Taylor found that the plaintiffs suffered “distinct, palpable, and substantial injuries” as a result of the TSP. She said the injuries are “concrete and particularized”, and not

---

204 Id. The U.S. Court of Appeals for the Sixth Circuit stayed the District Court’s ruling on October 4, 2006, while they considered an appeal by the government. Oral arguments for the appeal were heard on January 31, 2007.  
205 Id. at 18-20 (discussing defendants’ reliance on Laird v. Tatum, 408 U.S. 1 (1972)).  
206 Id. at 21.  
“abstract or conjectural.” Judge Taylor considered the following complaints made by the individual plaintiffs

- James Bamford, a journalist, author, and expert on U.S. intelligence, said his ability to research and write about the National Security Agency, intelligence and the War on Terror is “seriously compromised” by the TSP because sources are less likely to communicate with him for fear of government surveillance.\(^\text{209}\)

- Larry Diamond, a Stanford University Professor and c-editor of the *Journal of Democracy*, said his ability to “advocate and advise on democratic reform in the Middle East and Asia” is inhibited by the TSP because political dissidents are less willing to contact him for fear of government monitoring.\(^\text{210}\)

- Christopher Hitchens, a reporter and author, said that the TSP is a “detriment to his effectiveness as an investigative journalist” on Middle Eastern politics because individuals are “less forthcoming in their conversations with him,” due to the likelihood their communications are being monitored.\(^\text{211}\)

- Tara McKelvey, an editor of *The American Prospect* and *Marie Claire*, said the TSP “substantially impairs” her ability to communicate with Middle Eastern sources due to fears the communications will be intercepted.\(^\text{212}\)

- Barnett R. Rubin, Senior Fellow at the New York University Center on International Cooperation, believed the TSP interfered with his work as a scholar in exchanging controversial information and sensitive ideas with people in the Middle East.\(^\text{213}\)

- The members of the ACLU of Michigan argued that international calls to the Middle East were being intercepted and this surveillance inhibited members from “communicating freely and candidly” in their personal and professional communications.

- Noel Saleh, a member of the Michigan ACLU and a licensed attorney, said she has refrained from talking to friends abroad about topics that might trigger TSP monitoring. Saleh said that before he learned of the program, he felt free to engage in open


\(^{209}\) Id. at paras 147, 158.

\(^{210}\) Id. at paras. 159, 166.

\(^{211}\) Id. at para. 168.

\(^{212}\) Id. at paras. 174, 182.

\(^{213}\) Id. at paras. 13, 191.
communication about topics of the day. Saleh felt less able to discuss issues and gain insights with citizens of other nations.  

- Nabih Ayad, a member of the Michigan ACLU and a licensed attorney, said he will not have “certain kinds of conversations by phone” because he is afraid the government might be monitoring his communications in cases involving terrorist related immigration or crimes. On a personal level, Ayad avoided discussing certain political topics with family and friends for fear that the conversations will trigger monitoring.

- The Council of American-Islamic Relations complained that the TSP prevented members from furthering the mission of promoting public understanding of Islam because open communication of this nature might place the community under “unlawful surveillance.”

- Nazih Hassan, a member of CAIR-Michigan and a Lebanese immigrant, said awareness of the TSP has caused him to stop talking to family members about political topics and current events including “Islam and the war in Iraq, Islamic fundamentalists, terrorism, Osama bin Laden, al Qaeda, the war in Afghanistan and the riots in France and Australia.” Hassan said the TSP interferes with his ability to promote “peace and justice” in the United States through free and open communication. He is also unable to gain insight from people abroad on current events because he is fearful conversations on certain topics will trigger monitoring.

- Joshua L. Dratel, a criminal defense lawyer in New York and an expert on Military Tribunals, said that he has “ceased having certain kinds of discussions over the telephone or by email for fear that the government may be monitoring his communications.”

- Nancy Hollander, a criminal defense lawyer in New Mexico and a leader in recruiting volunteers to represent prisoners at Guantanamo, said the program has inhibited her communications with individuals in the Middle East for fear that the government might be monitoring her communications. She has decided to cease using phone communications to plan strategic or privileged aspects of her terrorism related cases.

- William W. Swor, a Michigan criminal defense attorney, says the TSP inhibited communications between himself and individuals in the Middle East. Since learning of the

---

214 Id., at paras. 77, 81, 82.
215 Id. at para. 90.
216 Id. at paras. 96, 102.
217 Id. at paras. 107, 110, 114-117.
218 Id. at paragraph 130, 135.
219 Id. at paras. 136, 141.
TSP, Swor avoided “certain kinds of discussions” by phone for fear the government might be monitoring his communications.220

**ACLU v. NSA: Developments**

The government appealed the *ACLU* decision to the Sixth Circuit Court of Appeals in Cincinnati where arguments were heard from both parties on January 31, 2007.221 On July 6, 2007, the Sixth Circuit Court of Appeals overturned the original ruling on the basis that the plaintiffs lacked standing to bring the suit against the government.222 Judge Alice M. Batchelder, in the majority opinion, said that the plaintiffs only alleged possible injuries from the government program.223 She said that although there was a possibility that the NSA was intercepting the plaintiffs’ communications, there was also a possibility that the agency was not intercepting the communications.224 Judge Batchelder said that the district court erroneously assumed the plaintiffs’ telephone and e-mail communications were “protected expressions” chilled by government surveillance.225 The appeals court found that the plaintiffs could only establish a “subjective chill.”226 The appeals court said that in order to establish a chilling effect the plaintiffs would have to show evidence beyond their knowledge of the government surveillance program.227 Judge Batchelder said due to the state secrets privilege, the plaintiffs

---

220 *Id.* at para. 142.


222 *Id.*

223 *Id.*

224 *Id.*

225 *Id.*

226 *Id.*

227 *Id.*
could not prove that they were the targets of the Terrorist Surveillance Program. Judge Batchelder, in the majority opinion, said

the plaintiffs do not — and because of the State Secrets Doctrine cannot — produce any evidence that any of their own communications have ever been intercepted by the NSA, under the TSP, or without warrants. Instead, they assert a mere belief, which they contend is reasonable and which they label a “well founded belief.”

Judge Batchelder, in the majority opinion, also said that the plaintiffs in the case who were attorneys said that surveillance interfered with their duty to keep attorney-client conversations confidential; she used this statement to say that the plaintiffs’ claim of harm was based on perceived harm to their clients, not themselves—and therefore invalidated the First Amendment claim. Judge Batchelder said District Court Judge Taylor wrongly interpreted the “chilling effect” precedent in the Laird case. She said the Laird plaintiffs alleged an actual personal fear of reprisal by the government, but the ACLU plaintiffs did not make this same claim.

In October of 2007 the ACLU appealed the case to the United States Supreme Court. The Supreme Court turned down the appeal on February 19, 2008, without comment.

228 Id.
229 Id. at 6.
230 Id.
231 Id.
232 Id.
CHAPTER 5
CONCLUSION

Telecommunications privacy and freedom is a complex issue that has developed over the 20th century as technology has expanded and intelligence agencies have worked to develop new initiatives in response to emergent threats to national security. At the dawn of the 21st century, the United States government struggled to balance concerns over protecting national infrastructure, with the inevitable encroachments on citizens’ civil liberties that these protections create.

Research was conducted to examine the connection between citizen’s First Amendment protections for free speech and Fourth Amendment protections for privacy. The balance between citizen’s constitutional protections for civil liberties and the government’s need to protect national security were examined. U.S. legislative, executive and judicial histories of domestic electronic surveillance were reviewed to detect patterns in government restrictions on citizen expression during times of national crisis. The effect of developing telecommunications technologies—as they relate to electronic surveillance capabilities—was also introduced as a variable in evaluating the balance between liberty and security.

This chapter will answer the research questions posed in chapter one by examining the findings from the data in chapters two through four. Future remedies for issues coming out of this research will be explored. Finally, future research recommendations for research will be presented.

This research was conducted to find answer for the following research questions:

- RQ1: What is the legislative history governing the surveillance of United States citizens?
- RQ2: What is the judicial history of the relationship between political surveillance of citizen communications and those citizens’ First Amendment rights?
• **RQ3:** How does the Fourth Amendment’s protection for privacy relate to the First Amendment’s protections for free speech?

• **RQ4:** Do current surveillance cases in the courts show a trend of protection for Emerson’s key First Amendment values, or a shift towards Lasswell’s garrison state?

• **RQ5:** What is the current balance between the need to protect civil liberties and the need to protect national security based on judicial interpretations of federal surveillance laws?

• **RQ6:** Does government surveillance of private communications create a chilling effect on free expression in the marketplace of ideas, as interpreted by the courts?

**Findings**

In this section, the research questions will be reintroduced and answers will be provided based on the data collected.

**What is Legislative History Governing the Surveillance of United States Citizens?**

Statutory provisions for electronic surveillance were created in response to technological advancements in the telecommunications industry and seek to balance government needs to protect citizens against citizens’ needs for civil liberty protection. The current body of law is neither unique from historical regulations, nor is it revolutionary in its scope. Congress has an established record for seeking to balance national security and civil liberties through warrant requirements for surveillance. Congress also has sought a balance between security and liberty by codifying legislative and judicial oversight for executive branch surveillance activities.

Domestic surveillance of citizen communications in the United States gained footing during World War I, when the State Department began intercepting and decoding messages transmitted within and beyond U.S. national borders. Two decades later, the Communications Act of 1934 addressed what was by then, a rapidly developing communications industry by enabling “rapid, efficient, nationwide, and worldwide wire and wire radio communication
service” for all people.¹ The Communications Act, for the first time, legally defined common carriers, wire communication, and foreign communication. The Communications Act encouraged cooperation between government and communication carriers in instances necessary to protect national security.²

The National Security Agency was the successor of Operation Shamrock, an early military operation to intercept telegraphic messages during World War II. The NSA was charged with protecting communications security, and obtaining foreign communications intelligence. The NSA has matured into an organization with a multi-billion dollar budget, overseeing domestic and foreign intelligence. Most operating details of the NSA are classified statutes protecting sensitive national security information.

Title III of the Omnibus Crime Control and Safe Streets Act, passed in 1968, was the first attempt by Congress to legislate government surveillance of private communications.³ The 1968 Omnibus Crime Control Act required warrants for government surveillance, except in specific situations such as protecting the nation from attack, obtaining foreign intelligence, protecting national security information, or protecting the government from violent overthrow. In addition to outlining judicial oversight for government surveillance, the Omnibus Crime Control Act updated the definition of wire communication to reflect the changing technical infrastructure of the telecommunications industry. The law also defined electronic devices and communications in light of these developments.

² Commc’ns Act, 47 U.S.C. § 210(b) (1934).
The Omnibus Crime Act made it illegal for common carriers to willfully disclose contents of intercepted transmissions, unless the disclosure was made to a government investigative agency and authorized by a written federal court order. The crime law also authorized 48 hours of warrantless surveillance when the government acts in an “emergency” to protect national security interests.

After the disclosure of illegal electronic surveillance by President Nixon during Watergate, the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities investigated national surveillance laws and practices.4 The resulting Church Committee report looked at cooperation between the government and private companies intercepting communications during World War II. The report’s revelation of gaps in national policy and laws governing surveillance was an impetus for future Congressional action addressing surveillance procedures.

The Foreign Intelligence Surveillance Act of 1978 (FISA) legalized non-criminal electronic surveillance within U.S. borders when probable cause could be shown that the purpose of the intercept was to collect foreign intelligence information. FISA also created the Foreign Intelligence Surveillance Court to review government applications for surveillance. Under FISA, the government was required to obtain a warrant from the court before spying on United States citizens within United States borders. The surveillance must be authorized by the Attorney General and is subject to congressional and judicial oversight. FISA also implemented minimization procedures to diminish the possibility that United States’ citizen’s communications would be intercepted. FISA permitted communication carriers to cooperate with the government

---

in providing intercepted communication contents as long as proper warrant and minimization procedures were honored.

The Electronic Communications Privacy Act of 1986 extended restrictions on the unauthorized interception of oral, wire and electronic communications by the government to include electronic communications. Communication providers were further restricted from disclosing the contents of communications to unauthorized third parties, requiring a search warrant for the interception of communications content, as well as subscriber records and service information. The law required the government to notify subscribers of interception within 90-days of the incident. Additionally, the FBI was granted the ability to use national security letters to compel providers to produce certain subscriber information.

The Communication Assistance for law Enforcement Act of 1994 extended legal requirements for cooperation between the government and private telecommunications companies, mandating surveillance-ready networks. Carriers were not only required to update networks and devices to accomplish this, they also were required to assist law enforcement in intercepting private communications when a warrant was provided. In emergency situations, carriers can intercept communications at their own discretion if a law enforcement officer demonstrates that a situation exists where national security is in jeopardy, or if there is risk of immediate danger, death or injury to a person. In these cases, a court order must be obtained within 48 hours of the interception.

After the 9/11 terrorist attacks, the PATRIOT Act of 2001 amended FISA to expand the government’s wiretapping powers. PATRIOT removed the FISA requirement that U.S. citizens

---


not be targeted, unless they were engaged in First Amendment activities, as long as foreign intelligence was a significant purpose of the investigation. PATRIOT allowed surveillance in new types of criminal investigations, such as terrorism, that were not included in FISA.
PATRIOT also legalized the sharing of information between federal law enforcement agencies in an attempt to promote collaboration between officers in protecting national security. Foreign intelligence information was expanded to include any information linked to protecting national security, even if it was linked to a United States’ citizen. PATRIOT allowed the use of roving wiretaps that did not specify a single target or location.

PATRIOT also allowed telecommunications carriers to voluntarily disclose customer communications to government agents when there was reason to believe that imminent death or injury might occur. If there was a reasonable belief that notifying the target would have an adverse result on the investigation, PATRIOT allowed the government to delay notification of surveillance.

The PATRIOT Act was amended in 2005, extending the original sunset provisions on certain sections of the original statute from 2009 to 2015. The PATRIOT reauthorization act of 2005 also required the Attorney General to provide additional information in his required annual reports. The types of offenses that are subject to surveillance were expanded to include new terrorism related crimes such as biological weapons, terrorist training and attacks, weapons of mass destruction, torture, and attacks on aircraft.

The PATRIOT Act was further amended in 2006 to clarify the use of national security letters. Under the 2006 amendments, letter recipients can petition a FISA judge, to appeal in the individual case, the letter’s nondisclosure requirements and judicial review is required within 72-hours of when the letter is served. In 2007, the Protect America Act further amended FISA,
removing the warrant requirement that foreign intelligence targets must be reasonably believed to be outside United States borders. The 2007 update also allowed the Attorney General to authorize intelligence for up to one year in cases where foreign targets are reasonably believed to be outside of the U.S. borders. Common carriers are required to provide the government with information, facilities and assistance necessary to intercept the suspected communication when a court order is presented. The person providing the information can be compensated for providing information, and failure to comply with an ordered request can result in the part being found in contempt of the court. Parties cooperating with the government are protected from legal action arising from the execution of the order.

The legal history of surveillance in the United States has developed alongside national concerns over growing security concerns. New agencies and laws have expanded the government intelligence infrastructure, as well as capabilities to address emerging threats to national security. The latest example of an expanded agency capability is the 2005 PATRIOT reauthorization act, which included new types of crimes that trigger warrantless surveillance. As laws have developed, Congress has been careful to attempt to codify safeguards for Americans’ civil liberties. Warrant requirements for domestic surveillance, judicial oversight, and quarantine of First Amendment activities are legislative protections to balance constitutional rights against the needs of the nation.

**What is the Judicial History of the Relationship Between Political Surveillance of Citizen Communications and Those Citizens’ First Amendment Rights?**

The Courts have traditionally addressed free speech against the backdrop of First Amendment protections intended to limit government interference with political participation. Justices have continually endeavored to limit the chilling effect that government action has on citizens’ abilities to inject new and subversive political views into the marketplace of ideas,
however the Court’s actual decisions reflect an understanding of government’s need to quiet dissent in times of national crisis. In *Schenck v United States*, the Supreme Court upheld the constitutionality of the Espionage Act on the basis that the defendant—in distributing literature that advocated against military enlistment—did not deserve First Amendment protection. The *Schenck* court found that the defendant’s actions in criticizing the draft posed a “clear and present danger” to the U.S. armed forces during a time of war. The Court said that although the defendant might have enjoyed constitutional protection for his expression during peace time, during war time the expression posed a unique danger—one of proximity and degree. From this reasoning, Justice Oliver Holmes established the “clear and present danger test” for judicial evaluation of government suppression of free expression.

The “clear and present danger” test established two criteria for allowing free speech. The first tier required unusual circumstances, such as the nation being at war. The second tier was the intent of the speaker—where he or she intended to incite action against the government. In the second tier of the test, the execution of a successful plan was not necessary, only the intent to commit a crime must be established. If both tiers of the test were satisfied, then the government could restrict free speech on the basis of national security. The Court upheld its *Schenck* ruling and the “clear and present danger test” in the 1919 cases of *Frohwerk v. U.S.* and *Debs v. U.S.*

In the *Abrams v. U.S.* case, decided in the latter half of 1919, the Court upheld the conviction of New York anarchists under the Espionage Act. In *Abrams*, the Court relied on

---

8 *Id.* at 252.
the “clear and present danger test” created in Schenck to find that only the intent of government overthrow was necessary to obtain a conviction under the Espionage Act, not the successful execution of a plan for overthrow. The Abrams case is most famous, not for its majority opinion upholding the need for intent as established in Schenck, but for the dissent of Justice Holmes, who had created the “clear and present danger test” in his majority opinion in the Schenck case. Justice Holmes, joined by Justice Brandeis, said that there should be greater protection for political speech. Holmes reasoned that the speech of the defendants in Abrams posed no true threat to the U.S. war effort. This was because there was no proof of “imminent danger.” Holmes said that the defendants’ words should be protected as free expression. The Holmes-Brandeis dissent in Abrams was not significant at the time of the decision, as it did not immediately impact the application of the clear and present danger test for the Abrams defendants. The Court would later draw on the reasoning of Holmes and Brandeis in the Gitlow and Whitney cases.

The next Supreme Court case, post Schenck, that would significantly change the Court’s approach to free speech cases involving potential state and local government infringement was the 1925 case of Gitlow v. New York,\(^\text{12}\) where the Court upheld the conviction of a defendant charged with advocating criminal anarchy. The Court upheld the constitutionality of the state statute, but most importantly, said the First Amendment applied to states through the Fourteenth Amendment’s due process clause.

In Gitlow, the Court did not use the “clear and present danger test” in its decision, although Justice Edward Terry Sanford, in his majority opinion, indirectly clarified the “clear and present danger” test created in Schenck and later expanded in Abrams. Sanford said that the

defendant’s publications advocated government overthrow through the “direct language of incitement.” He said it was not a philosophical abstraction, but a “sufficient danger of substantive evil.”

In *Schenck*, Justice Holmes had based the clear and present danger test on two criteria 1) circumstances surrounding the free expression, such as times of war or national crisis and 2) whether or not the defendant intended to incite a crime. The *Abrams* Court had recognized this standard, but Justice Holmes, in a dissent, said there must also be proof of imminent danger Rather than just a “clear and present danger.” Justice Sanford, in *Gitlow*, used the term “substantive evil” to describe the defendant’s words is a nod to the Holmes dissent in *Abrams* advocating greater protection for political expression unless there was a true threat to the nation.

In *Whitney v. California*, a 1927 case involving a California law criminalizing advocacy of violent or disruptive labor movements., the Court upheld the defendant’s conviction and said the constitutional protection for free speech did not confer an absolute right to “speak without responsibility.” In its holding, the Court majority did not apply the “clear and present danger test,” but rather decided the case on the fact that the statute did not criminalize mere advocacy, only violent or illegal actions. Justices Brandeis, in his concurrence, joined by Justice Holmes, emphasized that there must be evidence of “substantive evil” in order for government restrictions on free speech to pass judicial review. Brandeis said that the Court had failed to set a standard in the “clear and present danger” test for the level of substantive evil that was necessary to abridge free speech and assembly Brandeis argued that it must be a “substantial” level. Furthermore,

---

13 *Id.* at 665.
14 *Id.* at 667, 669.
16 *Id.* at 375-77 (Brandeis, J., concurring).
Brandeis said that “imminent danger” is not enough to satisfy the standards of the “clear and present danger” test. There must be some substantial “probability of serious injury to the state.” Although the majority opinion in Whitney did not significantly alter the application of the “clear and present danger test”, Brandeis’ concurrence would be mentioned in several Court opinions yet to come.

In the 1941 case of Bridges v. California, a case where the Supreme Court struck down the prior restraint of pretrial press coverage, the Court tightened up its standards in applying the “clear and present danger” test. The Court said that in order to pass the test and punish speech, the government must demonstrate that the defendant’s First Amendment activities posed a “substantive evil”, with an extremely high imminence. The Court relied on a new version of the “clear and present danger” standards established in Schenck, that there must be special circumstances surrounding the speech and the expression must be of a nature that would bring about substantive evil. The Court said previous cases decided on application of the “clear and present danger” test were recognition of only minimal protection for speech under the Bill of Rights. In order to restrict speech, the “substantive evil” must be 1) substantial, 2) extremely serious, and 3) highly imminent. In Bridges, the Court’s emphasis on a need for speech to pose “substantial” and “serious” harm, in essence, adopted the reasoning in the Holmes and Brandeis dissents of the previous decades.

In Dennis v. United States, decided June 4, 1951, the U.S. Supreme Court held that the defendants’ Smith Act convictions for Communist conspiracy to overthrow the government were not a violation of the First Amendment.17 Chief Justice Fred Vinson, in the majority opinion, said freedom of speech is not unlimited—dissenters do not have “unlimited, unqualified” rights

---

to speech—but rather speech must be weighed for its “societal value.” In *Dennis*, the Court wrestled with the meaning of the phrase “clear and present danger,” ultimately deciding that it did not mean the government had to wait for overthrow plans to succeed, rather it could intervene as soon as it learned of a plan. This removed the criterion of the need for an imminent danger, predicated on the success of a plan. This line of judicial reasoning was first mentioned by Justice Brandeis in his *Whitney* concurrence, and later established by the *Bridges* majority opinion.

In *Yates v. U.S.*, in 1957, the Court retightened the government’s burden of proof that had been relaxed in *Dennis* and found that people must be encouraged to do something for there to be a violation of the Smith Act. Only advocacy of action could be criminalized, not an idea alone. The Court said that advocacy and teaching of subversive ideas were not illegal as long as they were advanced as abstract principles and not incitement of violence. The *Yates* holding reaffirmed the clear and present danger test relied on before the holding in *Bridges v. California*.

Twenty years after the *Yates* decision, the Court would again review the application of the “clear and present danger” test in the 1969 case of *Brandenburg v. Ohio*. In Brandenburg, the Court affirmatively overruled the *Dennis* holding and said that the “clear and present danger” test required strict evidence of “imminent danger.” In the case, which involved a KKK rally, the Court struck down an Ohio Criminal syndicalism statute as unconstitutional through the Fourteenth Amendment’s extension of First Amendment standards for state actions. The Court said that the “clear and present danger” test required the government prove three criteria before restricting free expression: 1) intent to promote unlawful actions 2) imminence—not required by the *Dennis* Court’s interpretation of the “clear and present danger test”—and 3) likelihood. The

---

18 Id. at 503

*Brandenburg* decision emphasized a need for a showing of imminence—a departure from the bad tendency test formed in *Whitney*—and it more strictly defined a rigorous standard for the likely success of advocacy in the time period following incitement.

In the 2003 case of *Virginia v. Black*, the Court struck down a Virginia statute banning cross burning as unconstitutional under the First Amendment. The Court said Black—in burning a cross on private property with the permission of the owner—did not intend to intimidate passersby who witnessed the act. The Court added that First Amendment protections for speech are not absolute and certain categories of speech “may” be regulated. In striking down the Virginia statute, the Court broadened First Amendment protections in the application of the “clear and present danger” test by renewing the standard that restricted actions must be evaluated on the speakers’ “intent.” This reintroduced a standard for “intent” established in *Dennis*, where the Court said that “the intent to overthrow the Government of the United States by advocacy” amounted to intent to “deprive” others of constitutional rights. The *Virginia* case in some ways introduced doubt in interpreting the Court’s *Brandenburg* decision that created three new criteria for the test.

Historically, government surveillance of citizens involved in political dissent was conducted through the monitoring of publications, speeches and membership lists of subversive organizations. Although the First Amendment protects political speech, the Supreme Court has recognized a need for the suppression of expressions that pose a threat to national security. The Court first used the “clear and present danger” test to evaluate expressions targeted by the government in criminal statutes during the early part of the 20th century. The test did not require likelihood of a expression’s success in harming the government, although Justices Brandeis and

---

20 *Dennis*, 341 U.S. at 500.
Holmes introduced a need for this criteria in their dissenting and concurring opinions of the era. The need for likelihood was adopted by the Court in Brandenburg, where it reinterpreted the “clear and present danger” test. The Brandenburg test requires the government to prove that the expression 1) has the intent to promote unlawful actions, 2) is imminently likely to result in immediate danger to the nation, and 3) has a high likelihood of successful execution. The judicial application of the Brandenburg test to evaluate political dissent in times of national crisis may prove a good model for evaluating current government surveillance of targets engaged in political dissent via telephone communications. This is due to the role of the telephone in modern society as a tool enabling a geographically diverse populace to engage in a national marketplace of ideas.

If the government uses domestic electronic surveillance to monitor and punish expression that is part of a political dialogue—necessary to promote free exchange in the market—then the surveillance programs might be best evaluated by the application of the Brandenburg test. The courts have traditionally used the Fourth Amendment’s standards for search and seizure to evaluate government surveillance of citizens. Therefore, there is no direct case law that applies the First Amendment standards to electronic surveillance. However, contemporary technological advancements in the telecommunications industry, as well as citizens’ increased reliance on this new tool for political dialogue, could be seen as impetus for applying the First Amendment’s higher standard of judicial scrutiny in cases involving free expression.

**How Does the Fourth Amendment’s Protection for Privacy Relate to the First Amendment’s Protections for Free Speech?**

The First Amendment protections for free expression and the Fourth Amendment protections against unreasonable search and seizure exist in a symbiotic nexus, designed to protect not only home and property, but also ideas and expression. The Courts have repeatedly
examined the nature of the use of communications networks by citizens to create the current assumption that the telephone is essential to private life and public expression.

Chapter three provided a comprehensive account of the major Fourth Amendment cases involving surveillance and Fourth Amendment protections for citizens’ communications. In answer to this research question, the data has been condensed to exclusively highlight instances where First and Fourth Amendment protections collide. Although these issues were not critical to the decisions in the cases—and often the data presented here relies on concurring and dissenting opinions—the examination of the judges’ thoughts on surveillance in regard to civil liberties is valuable for no other reason than the rarity of this type of analysis by the courts. Furthermore, this analysis reveals how the Court has historically viewed telecommunications—at first a novelty and later and essential tool for citizen dialogue.

The court opinions involving electronic surveillance address the Fourth Amendment right to privacy, yet many also hint that First Amendment protections for citizen communications exist as well. The judicial holdings will be summarized in this paragraph, before each decision is reviewed individually. In the 1928 Olmstead v. United States opinion, the Supreme Court found that warrantless wiretapping violated Fourth Amendment constitutional protections against unlawful search and seizure. The 1942 Goldman v. United States case dealt with developing technology to bug a conversation from a neighboring room—this was found to be legal under Fourth Amendment protections since it did not involve actual trespass. In the 1963 case Lopez v. United States, the Court upheld the standard that no trespass meant no violation of Fourth Amendment protections, even if recording devices were used to intercept communications intended to be private. The 1967 Katz v. United States opinion reversed the trend of Goldman and Lopez, requiring a warrant to intercept communications. In the 1972 Keith case, formally
known as United States v. United States District Court, warrant requirements were extended to
domestic surveillance cases. In the 1975 Zweibon v. Mitchell case, warrant requirements were
extended to domestic organizations.

In reviewing the Fourth Amendment protections provided in the judicial history, many
threads of First Amendment theory can be found that relate to free speech and electronic
surveillance. The opinions also reveal a judicial history that paints the Court’s view of wire
communications (later to become electronic communications) and surveillance. In the Olmstead
Case, the Court upheld the conviction of plaintiffs convicted using evidence obtain by inserting
small wires in the basement of the building to intercept communications. The Court found that
tapping phone conversations was not an unlawful search and seizure because the telephone
system was not operated by the government in the same way as the U.S. postal system.
Additionally, the postal system transmitted letters—personal effects—whereas wire
communications were transmitted to the “whole world.” The Court viewed electronic
interception as simply hearing this transmission. The Court compared phone lines to highways.

The dissenting justices in the Olmstead opinion had different views that foreshadow the
future judicial standard for looking at electronic surveillance and the nature of
telecommunications. Justice Brandeis viewed the telephone as an instrument unimaginable to the
forefathers when they wrote the Constitution. He predicts a day when the government might be
able to reproduce documents in court without removing them from “secret drawers.” Brandeis
saw no difference between mailed letters and phone communications, emphasizing that the
framers sought to protect Americans “in their beliefs, their thoughts, their emotions and their
sensations.” Justice Holmes’ dissent also offers an early 20th century interpretation of phone
communications: “The contracts between telephone companies and users contemplate the private use of the facilities employed in the service.”

In *Lopez v. United States* (1963), the Court upheld a Massachusetts’ conviction of a man for bribery of an IRS agent. The evidence used in the conviction was obtained through wiretapping, but the Court found that the agent’s use of a microphone only enabled him to record a conversation that he was already party to, therefore he was not trespassing in his search and seizure. Justice Brennan railed against this reasoning in his dissent:

> If a person commits his secret thoughts to paper, that is no license for the police to seize the paper; if a person communicates his secret thoughts verbally to another, that is no license for the police to record the words.”

Brennan added that the only way to guard against contemporary eavesdropping is to “keep one’s mouth shut,” much different than conventional tactics of “lowering voices.”

In harking back to the majority’s reliance on the *Olmstead* decision, the dissenting justices argued that modern life necessitates the use of the telephone as a valuable tool in “free human communication”—just as valuable as communication that takes place solely within the confines of the home. He added that electronic surveillance makes the police “omniscient,” in effect a tool of tyranny. Brennan wrote that electronic surveillance was a weapon that strikes at “freedom of communication.” Brennan said free speech is undermined if people fear to speak “unconstrainedly” in the privacy of their own home or office.

---


23 Id. at 453.

24 Id. at 466.

25 Id. at 470.

26 Id. (citing Donald B. King, *Wire Tapping and Electronic Surveillance: A Neglected Constitutional Consideration*, 66 DICK. L. REV. 17 (1961)).
In *Berger v. New York* (1967), the Court overturned a lower court decision upholding the conviction of a man under a New York eavesdropping statute allowing general searches, which do not name a specific place or person in the warrant. The court likened wiretappers to eavesdroppers of the past, adding that “Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.” Justice Douglas likened warrantless surveillance to British general warrants, which helped to spur the American Revolution. He added that electronic surveillance without warrant requirements amounts to an illegal dragnet putting an invisible policeman in every home. He sees this as moving America closer to a “totalitarian regime,” where “Big Brother” intrudes into the lives of everyone.

In the *Keith* case, the Court affirmed the lower court decision requiring warrants to monitor telephone conversations, even in cases of national security. In highlighting the “convergence of First and Fourth Amendment values” unique to surveillance, the majority of the Court found that protecting politically unpopular speech is a constitutional priority, especially in cases of domestic security: 

"Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect ‘domestic security.’"

---


28 General search warrants allow an officer to conduct a search that does not specify a particular place or person. General search warrants were used by the British and were called writs of assistance. Writs of assistance, which helped tax authorities search merchant imports for illegal and unclaimed goods. The legality of writs of assistance was affirmed in the Townshend Acts, passed by the British Parliament in 1767. *See generally* Robert J. Chaffin, *The Townshend Acts of 1767*, 27 WM. & MARY Q. 90, 90-121 (1970).

29 *Berger*, 388 U.S. at 63.

30 *Id.* at 68 (Douglas, J., concurring).


32 *Id.* at 314.
In *Keith*, Justice Powell said that vigorous private dissent by citizens is “essential” to a free society. The Court’s decision recognized the Fourth Amendment’s protections of privacy, as it relates to the free exercise of First Amendment rights of free speech, by recognizing citizens’ expectation of privacy in their home and communications.

The Courts have traditionally decided cases involving government electronic surveillance on the Fourth Amendment prohibition on warrantless search and seizure. In the 1965 case of *Griswold v. Connecticut*, the Court recognized the individual right to privacy as an unnamed “penumbra” right inherent in the Bill of Right’s First, Third, Fourth and Fifth Amendments. The “individual right to privacy” would quickly take hold in the Court’s language used in opinions involving government surveillance of private communications. In the 1967 *Berger* opinion, Justice Clark recognized that wiretapping techniques were spurring Congress to create statutory protections for “individual privacy.” In the 1967 *Katz* opinion, Justice Stewart said the telephone played a “vital role” in private communication. In the 1972 Keith case, Justice Powell said the Omnibus Crime Act of 1968 was an attempt by Congress to protect “the privacy of individual thought and expression.”

Although the Court has recognized a need for privacy in telephone communications, it has not acknowledged the role of the telephone in the marketplace of ideas. Privacy is not protected under the First Amendment. However, given the Court’s recognition of the individual right to

---

33 *Id.* at 315.

34 *Berger*, 388 U.S. at 49.


36 *Keith*, 407 U.S. at 301.
privacy emanating from the Bill of Rights, it could be a relevant factor in cases involving private
communication on political matters.

**Do Current Surveillance Cases in the Courts Show a Trend of Protection for Emerson’s
Key First Amendment Values, or a Shift Towards Lasswell’s Garrison State?**

Contemporary court cases filed in response to The Terrorist Surveillance Program are a
good starting point for evaluating current judicial sentiment towards protecting citizens’ First
Amendment rights in response to government surveillance. The allegations made by plaintiffs in
the cases will be analyzed using Emerson’s values inherent in protecting the First Amendment.
Then, the government actions under the Terrorist Surveillance Program will be analyzed using
Lasswell’s standards for protecting national security.

Emerson’s first value in protecting the First Amendment was that it assures individual self-
fulfillment. 37 Emerson said that expression was an “integral part” of mentally exploring ideas
and forming opinions. 38 In *Hepting v. AT&T*, Carolyn Jewel said she avoided discussing U.S.-
Iraq policy with an international acquaintance. In the *ACLU v. NSA* case, Nazih Hassan stated
that he avoided discussing controversial topics with family members in order to avoid triggering
monitoring. Both of these assertions, if true, demonstrate the potential for the Terrorist
Surveillance Program to interfere with self-fulfillment. Discourse, particularly on current and
controversial events, is critical to the need for individuals to grow mentally through discussion of
human issues and the discovery of new ideas. The second value Emerson identified was
promoting the discovery of truth. 39 Emerson said free expression played a “vital social role” in

---

37 EMERSON, supra note 18.

38 Thomas I. Emerson, supra note 6.

39 EMERSON, supra note 18.
marketplace by promoting citizen discourse and dialogue.  

In *ACLU v. NSA*, Christopher Hitchens, Tara McKelvey and James Bamford, all journalists, claimed that the Terrorist Surveillance Program interfered with their ability to act as journalists. They said potential sources are afraid to contact them because the communication might be intercepted under the TSP. The journalists contend that if they are unable to obtain information about important public issues, they will be prevented from discovering “truth” as they try to act in a “watchdog” role, protecting citizens from government.

Emerson’s third value inherent in First Amendment protection was the ability by all members of society to participate in decision-making. Emerson said this participation was “indispensable” to the American form of representative government. In *ACLU v. NSA*, Larry Diamond said he was unable to advocate and advise on democratic reform in his role as a journal editor because political dissidents were now afraid to contact him. Barnett Rubin said his work as a scholar has been obstructed because he feels inhibited when “exchanging controversial information” with people in the Middle East. Emerson understood the First Amendment as a protection for citizens when participating in the marketplace of ideas. Scholars and editors claim their ability to participate in international diplomacy is stifled by the Terrorist Surveillance Program. This may indicate the program is working against Emerson’s key value protecting participation in the political decision-making process. Promoting social stability through discourse is the final principle identified by Emerson as fundamental to the First Amendment’s purpose.

In the *CCR v. Bush* case, the attorneys named in the complaint said they have altered

---


41 *Id.*

42 *Id.*

43 *Id.*
their relations with “suspect” clients in order to avoid government monitoring. One plaintiff said that she now travels outside of the country in order to meet confidentially with her client. If, as the attorneys claim, basic legal activities such as discovery and deposition must now be conducted under a veil of secrecy, it would appear that the Terrorist Surveillance Program might undermine social stability. If citizens and attorneys, as they claim, are forced to operate outside this marketplace in discussing controversial topics—due to a fear of interception—then the system of justice could be circumvented as a tool for societal change. The Terrorist Surveillance Program might then be seen as at odds with Emerson’s key value of free expression promoting social stability.

Harold Lasswell, in his book *National Security and Individual Freedom*, discussed the centralization of power and the prevalence of security measures during times of crisis. Lasswell presents a multi-step model of how citizens and government interact in a shift towards a more totalitarian style of government. Lasswell’s steps and examples are used to analyze the Terrorist Surveillance Program to determine if increased domestic surveillance poses a threat to constitutional protections for individual rights to free expression. Only the first three of Lasswell’s four principles will be analyzed since the fourth deals strictly with the economy and is beyond the scope of this article.

Lasswell’s first principle governing national security programs stipulated that elite security programs are a threat to the tenet of civilian supremacy in our system of government. The Terrorist Surveillance Program, though authorized by the executive branch, operated beyond the oversight of the American electorate, without judicial oversight. The National Security Agency,

---

44 LASSWELL, supra note 36.

45 Id.
instead of being accountable to civilian representatives and judges, was under the supervision of generals and often works with military intelligence. This might activate the military garrison model—where intelligence agencies operate beyond judicial review—Lasswell advanced in his theory.

Lasswell’s second principle governing national security programs stipulated that there should be a free flow of information in a Democratic society. Under the Terrorist Surveillance Program, interception of communications was conducted in secret. A citizen, due to the states secret privilege and the use of national security letters, might never learn they were the target of surveillance. There is no way for a citizen to make a successful Freedom of Information Act request and discover a pattern of suspicious activities because intelligence activities are classified. As executed, the TSP operated entirely beyond the view of citizens.

Lasswell’s third principle governing national security programs identified danger to the civil liberties of the individual. This is the principal most strongly called into question by the Terrorist Surveillance Program. Lasswell said that free expression was the most important guarantee made by the Bill of Rights. He said free expression promoted the political process. Citizens must be free to discuss the issues of the day, both within the national borders and beyond them. If attorneys and scholars, as they claimed, avoided discussing important national issues, then the Terrorist Surveillance Program might pose a threat to individual civil liberties, as explained in Lasswell’s third principle.

The Terrorist Surveillance Program might also be evaluated against Supreme Court Justice William Brennan’s factors that lead to the infringement of civil rights during times of crisis.

\[46\text{ Id.} \]
\[47\text{ Id.} \]
Brennan said the government, during times of crisis, is more likely to infringe on civil liberties when 1) the crisis creates a national fervor, 2) security risks are exaggerated and 3) the perceived risks results in a forfeiture of civil liberties until the risk subsides.\(^{48}\) The Terrorist Surveillance Program was initiated during the “national fervor” following the 9/11 terrorist attacks on the World Trade Center in New York. Security threats leading to the authorization of the TSP could have been exaggerated, based on uncertainty. The perceived risk of terrorism resulted in changes to electronic surveillance laws that lessened protections for civil liberties. These findings are not conclusive in establishing an infringement on civil liberties, but the Terrorist Surveillance Program was created in a time of national fervor that is still underway in the War on Terror. Therefore the applicability of the latter two prongs of Brennan’s criteria for an infringement cycle might only be evaluated accurately once the fervor has died down and law makers are able to evaluate the true security risks that existed.

The narrow nature of this research project and the nature of the legal research itself means that a conclusive answer to question four is not possible. However, the evidence from this project shows that the TSP is at least in some ways incompatible with Emerson’s First Amendment values and consistent with concerns Lasswell had about governments tending toward authoritarianism.

**What is the Current Balance Between the Need to Protect Civil Liberties and the Need to Protect National Security Based on Judicial Interpretations of Federal Surveillance Laws?**

The shifting balance between the needs to protect civil liberties versus national security create pendulum-like swings in United States surveillance policy, alternating between periods of heightened attention to the competing needs. Contemporary surveillance issues are not unique;

\(^{48}\) *Id.* at 1375.
nor do they create an emergent situation that merits a complete reinterpretation of constitutional protections. They are simply a paradigmatic shift in national sentiment.

There is a parallel between the current War of Terror and the Communist Scares experienced during the 20th century. In looking at the history of U.S. surveillance, cycles emerge revealing a shifting balance between the need to protect civil liberties and the need to protect national security. This research has drawn from examples and created comparisons to past eras where the federal government has been heavy handed in its protection of security to the detriment of citizen’s rights.

Building on Lasswell’s ideas and the right to express unpopular political beliefs, the research explores the significance of President Bush’s underlying message that “You are either with us or against us” in the War on Terror. This type of language seems to indicate that dissent from government endorsed positions could be seen as the type of behavior prohibited in both the Alien and Sedition Acts, as well as the Smith Act. The Smith Act of 1940, which criminalized advocacy of violent government overthrow, is still part of the United States Code.

The Bush administration argued that the War on Terror was a different kind of war—as a result, the Terrorist Surveillance Program has been seen by the administration as a program built on this principle. In testimony before the Senate Select Committee on Intelligence in 2002, former NSA Director Michael Hayden suggested the September 11th attacks would drive the nation “more toward security.” Hayden also suggested the attacks were cause for a reevaluation of the


51 Hayden Statement, supra note 22.

52 Id.
balance between security and individual freedoms. After the attacks of September 11th, the theme of protecting “national security” became commonplace in political rhetoric, media accounts and public sentiment. The Bush Administration said the Terrorist Surveillance Program was a way to address emergent national security concerns and issues related to terrorism. The War on Terror might reshape how society balances civil liberties against needs to protect national security.

Terrorism has become a principal factor in the handling national security concerns. At the same time, advancing telecommunications technology has changed laws addressing electronic surveillance. Where to draw the line between security and liberty depends on the convergence of the two bodies of law governing national security and liberty from arbitrary exercise of authority. The executive branch has interpreted existing legislation to protect national security interests over personal liberty. This reflects a cyclical give and take between security and privacy. In times of war, people may be more willing to sacrifice liberty. In times of peace, civil liberties are afforded greater importance. The current national debate over existing surveillance laws is a progression of the cycle and affords Congress an opportunity to clarify their intentions in regulating domestic surveillance.

**Does Government Surveillance of Private Communications Create a Chilling Effect on Free Expression in the Marketplace of Ideas, as Interpreted by the Courts?**

The value in protecting citizens’ First Amendment rights is evident in an examination of court decisions involving politically subversive speech, as well as cases involving domestic

---

53 Id.


55 Risen & Lichtblau, *supra* note 5.
electronic surveillance. When citizens change the contents of their communications to evade government action, the “chilling effect” is realized, whether or not their perception is accurate.

Many First Amendment issues arise in the examination of the Supreme Court cases involving electronic surveillance, as well, specifically the chilling effect and breathing space. “Chilling effect” refers to a government action that curbs a citizen’s ability or desire to engage in First Amendment protected activities. “Breathing space” refers to a theoretical buffer zone that protects citizens from oppressive governmental control. These concepts have traditionally been applied in analyses of free speech and expression, as opposed to protection of citizens against government surveillance. Technological developments spurring communication over private networks make the two principles relevant to the debate over First Amendment rights involved in electronic surveillance. An examination of federal court opinions and the sentiment of the judges who authored opinions (majority, concurring and dissenting) in these important cases, can help develop theory that might help protect citizens from overly intrusive government electronic surveillance.

The chilling effect stems from the judicial doctrine for a marketplace of ideas for speech, a doctrine akin to the economic marketplace. In 1919, in *Abrams v. U.S.*, the Supreme Court coined the phrase “marketplace” in a case involving prosecution under the Espionage Act of 1917.56 Previously that year, the Court had upheld another conviction under the Espionage Act in *Schenck v. United States*.57 That opinion labeled the acts of challenging the conscription system as a “clear and present danger” to national security. In *Debs v. U.S.*, labor lead Eugene V. Debs challenged the military in a Socialist political speech and was later arrested and his conviction

upheld by the Supreme Court in 1919.\footnote{Debs v. United States, 249 U.S. 211 (1919).} The Court, in its opinion found that obstructing the draft was a clear and present danger to military operations.

In 1925, \textit{Gitlow v. New York} extended First Amendment protections to the states through the Fourteenth Amendment’s due process clause. However, in \textit{Gitlow}, the Court acknowledged that speech could be restricted when it posed a “substantive danger” to national security. The 1951 decision in \textit{Dennis v. United States} upheld the controversial Smith Act of 1940, which prohibited speech advocating forceful overthrow of the government. In \textit{Dennis}, the Court expanded the Smith Act to include the intention to overthrow the government in the test to determine clear and present danger. In the 1957 \textit{Yates case}, the Court backed off of its \textit{Dennis} holding and found that ideas alone could not be criminalized in the absence of advocacy of violence. The \textit{Dennis} case was decided during the McCarthy era of government action against Communist organizations and sympathizers. The Court lessened the \textit{Dennis} provisions in the 1957 \textit{Yates} case by overturning the convictions of Communist sympathizers. The Court held that advocacy of action alone was not enough to trigger criminal prosecutions, there must also be an incitement to violence against the nation.

The Court wrestled with constitutional protections for free speech in its creation and application of the “clear and present danger” test, but the first time the Court acknowledged a potential for the “chilling” of free expression due to government restrictions was in a case involving freedom of association. In the 1919 case of \textit{Dombrowski v. Pfister}, the Court said a Louisiana law—requiring members of subversive political organizations to register with the government—created a “chilling effect” on First Amendment rights. The Court said that the
statute had the potential to create a “danger zone” where protected expressions “may be inhibited.”  

Lamont v. Postmaster General was a 1965 Supreme Court case involving government restrictions on distribution of communist propaganda. The majority opinion said the Postal Service and Federal Employees Salary Act of 1962—requiring registration in order to receive communist themed mailings—was an unconstitutional abridgement of citizen’s First Amendment rights. In his concurring opinion, Justice Brennan said a law like the 1962 Act could result in a “barren marketplace of ideas.”

The Court also has never decided a case involving electronic surveillance on the basis of a need for breathing space in the marketplace of ideas. “Breathing space” is the insular buffer around the marketplace of ideas that is necessary to prevent a “chilling effect” on constitutionally protected activities. Whereas the “chilling effect” refers to government regulation that has the tendency to intentionally or unintentionally curb politically speech, “breathing space” refers to the public need to be able to discuss a wide range of political and social issues from a broad range of perspectives. Even if ideas and proposed solutions to problems are not popular or “correct” for some aspect of the audience, the argument for adequate “breathing space” is that the wide-ranging discussion of ideas and proposed solutions promotes democracy.

The Court introduced the need for “breathing space” as a condition for free debate and expression in society in the 1964 case of New York Times Co. v. Sullivan, where it struck down an Alabama libel law as unconstitutional. The Court said that political criticism needs


“breathing space to survive.” The 1974 case of Gertz v. Welch is significant because the Court held that the First Amendment permitted statutes that formulated their own standards of libel for defamatory statements made upon private figures, as long as liability is not imposed without fault.\(^{62}\) Equally significant in a discussion of breathing space is the dissenting opinion of Justice Brennan who added to the concept of breathing space by saying that there must be “breathing space” for free and robust debate.\(^{63}\) Brennan said First Amendment expression needs “elbowroom” to flourish.\(^{64}\)

The idea of breathing space was mentioned briefly in two late 1980’s cases involving defamation. The Court, in the 1986 case of Philadelphia Newspapers v. Hepps, extended “breathing space” protections to speech on political matters of public concern. The Court found that even if defamatory speech about public officials was false, there should be breathing space for its First Amendment expression. The Court cited the Hepps decision in the 1988 case of Hustler Magazine v. Jerry Falwell, finding that a parody of a public figure—even with falsehoods depicted—warranted “breathing space” for First Amendment expression.

The judicial treatment of free speech depends upon national security concerns prevalent in the country at the time of the decision. When there are legitimate concerns to the smooth operation of government—such as the cases involving resistance to the military draft during times of war—the Court tends to permit more government restrictions on speech. For example, social activist and presidential candidate Eugene Debs was jailed for his public statements against military operations. However, when citizens’ political ideas—as opposed to actions—are chilled by government restrictions on the breathing space needed in the marketplace, the Court is

---


\(^{63}\) Id. at 361 (Brennan, J., dissenting).

\(^{64}\) Id. at 367.
more inclined to side with free speech concerns. For example, the Louisiana law requiring political subversives to register with the government was invalidated, as was the 1960’s requirement for communist sympathizers and supporters to register with the postmaster in order to receive mailings from certain organizations. This attention to clear and present danger seems to reflect a line of reasoning in the Court that citizens should be able to explore politically unpopular ideas, as long as they do not take actions to undermine national security.

Several Supreme Court justices allude to the chilling effect of electronic surveillance—if not by name—in cases decided on Fourth Amendment grounds. First, select cases from chapter two will be highlighted to show the Supreme Court’s recognition of telephone communication as part of the marketplace. Cases are also highlighted if they seem to suggest the Court’s acknowledgment of a “chilling effect” or “breathing space.”

In the 1928 case of *Olmstead v. United States*, the court majority upheld the Fourth Amendment legality of tapping private phone conversations. In his dissent in *Olmstead*, Justice Brandeis discussed the motivations of government wiretapping and said “dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.”

Brandeis was acknowledging the tendency of government officials to restrict speech in the name of national security—at the cost of political free expression in the marketplace.

In the 1961 case of *Silverman v. United States*, the Court majority described the government’s action of placing a microphone inside a target’s home as an “actual intrusion into a constitutionally protected area.” Although the *Silverman* Court did not mention the marketplace, their reference to a “constitutionally protected area,” could be a nod to the breathing space insulating First Amendment activities.

---

Brandeis in his dissenting opinion in the 1963 case of *Lopez v. United States*—where the majority upheld government surveillance—said that electronic surveillance undermined freedom of speech when people were afraid to speak “unconstrainedly” in their private homes or offices.\(^6^7\) In the 1967 case of *Berger v. New York*, the court extended Fourth Amendment guarantees against warrantless search and seizure to conversations. The Court said that a state statute permitting warrantless surveillance would be a government “dragnet” that placed an “invisible policeman” in every home. The Court said this might lead the country closer to a “totalitarian regime.”\(^6^8\) Douglas argued for a “high constitutional barricade against the intrusion of Big Brother into the lives of all of us.”

More recently, the plaintiffs in the *ACLU v. NSA* case, filed in January of 2006, allege that the Terrorist Surveillance Program had a chilling effect on their activities protected by the First Amendment. Judge Anna Diggs Taylor, of the Eastern United States District Court of Michigan, found for the plaintiffs and based her decision in part on the chilling effect of the governments’ program. The Sixth Circuit Court of Appeals overturned the cases finding the alleged “chilling effect” was subjective.

The Supreme Court has never decided a case on the basis of the chilling effect, although District Court Judge Walker did acknowledge the chilling effect of surveillance in her holding in the *ACLU* case. As Daniel Solove pointed out in his 2007 *New York University Law Review* article, First Amendment protections should restrict government information gathering if there is a “discernible” chilling effect on constitutionally protected activities.\(^6^9\) However, this chilling


effect can be difficult to establish beyond a “person’s own assertions that she was chilled.” The Sixth Circuit Court of Appeals decision in the ACLU case might reflect judges’ hesitance to recognize a chilling effect in electronic surveillance.

**Analysis of Findings**

Changes in technology have spurred the development of electronic surveillance law. In the early twentieth century, the telegraph was merely a series of start and stop switches that allowed the transmission of electrical pulses. From this crude beginning, the telephone developed to allow people to exchange actual words over the wires that had previously hosted the electrical impulses. Early telephones ran on circuits, which rang all connected callers—under this model eavesdropping was common. In the 20th century, telephones have evolved into a private form of communication where words are exchange over wire lines presumed to be secure from eavesdropping.

The telephone is used in lieu of face-to-face communication in the marketplace of ideas. It is used to facilitate family affairs, business transactions, but most importantly, it is used to interact with other citizens through political discourse and exchange. This latter use of the telephone has experienced varied forms of restrictions, notably centered around times of war and national unrest. There is always a shift away from protecting civil liberties and towards protecting national security during these periods. In the early part of the century this shift spurred the beginning of military spying operations such as the Black Chamber. During the Communist Scare of the 1950’s it was impetus for the creation of the National Security Agency. In the 1960’s, political uprisings and civil rights movements, led Congress to pass the Omnibus

---

70 *Id.*
Act, which facilitated domestic spying on citizens. In the 1970’s, following Watergate, Congress passed FISA in response to concerns over spying by the executive branch.

The current War on Terrorism, and the resulting PATRIOT Act and revisions, are simply the latest wave of legislation to address the cyclical shift in this balance between national security and civil liberties. Different administrations have unique views based on their interpretation of existing laws during times of crisis. Likewise, citizen response to contemporary surveillance initiatives is dependent upon the crisis at hand and the perceived risk to citizens’ well being. Electronic surveillance and wiretapping are “intrusive forms of investigation” that should be used in “limited and unusual circumstances.”\(^{71}\) These tactics might be counterproductive to protecting the First Amendment activities of citizens.

Historically, national politics, events and sentiment have redefined the line between negative liberty and security. The drive to eradicate terrorism is simply the latest initiative in a long line of developments that have shaped the electronic surveillance policies of the United States government.\(^{72}\) Many of the changes in intelligence gathering implemented since the passage of FISA reflect not only the new threat of terrorism, but also the previously discussed technological changes that have led to the rapid expansion of the telecommunications industry.

The government, in asking AT&T to disclose customer communications under the Terrorist Surveillance Program, may have engaged in the same practice used to intercept telegraphic messages during WWII. In each of these time periods, the national security crisis influenced the government-industry relationship. The 1917 telegraph intercepts occurred during World War I. The intercepts under Operation Shamrock came during World War II. The AT&T

---

\(^{71}\) ELECTRONIC PRIVACY INFORMATION CENTER & PRIVACY INTERNATIONAL, PRIVACY AND HUMAN RIGHTS 2001: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (2002).

case stemmed from the national crisis surrounding the War on Terrorism. The current
government-industry relationship is unique from past arrangements in that it is entrenched in a
legal framework that has developed since the 1947 National Security Act.

The current situation is characterized less as a “surveillance” society and more of a society
that is “monitored.” Beginning as a wartime defense strategy, the surveillance of
telecommunications networks has organically evolved to allow for the constant monitoring of all
citizens. In that citizens feel they are always being observed in their communications, they are
cautious and less likely to engage in activities that could be seen as illegal or arouse suspicion
from authorities.

How courts ultimately rule on the legality of the program will directly influence where the
line is drawn between liberty and security. If this current climate of secrecy surrounding
electronic surveillance continues, then it seems, indeed, a new privacy paradigm will be
advanced. U.S. citizens have already indicated their reluctance to speak up against government
surveillance programs designed to protect them from enemy plans in the War on Terror. If
Therefore, there seems to be a new legal paradigm for privacy where citizens are complacent and
willing to sacrifice their personal privacy to feel safe in a world threatened by terrorism or other
unknown enemies.

Hence, the TSP acts as an informal system of prior restraint on free expression. This
seems to make a mockery of the First Amendment, which was created by men who believed that
speech should be free from prior restraint. As Justice Brandeis said in Whitney v. California,

\[^{73}\text{See Ch. 1 polling data, supra.}\]
“Those who won our independence… believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth.”

The citizens discussing terrorism over communication networks have committed no crime beyond contemplating an alternative to Democracy. Though advocacy might be punished in a public sphere, these citizens are simply discussing issues in the private realm of correspondence. The rationale of the Administration in authorizing the TSP was to protect the country, yet the program seems to have threatened citizen involvement in the marketplace of ideas. However, scholars, politicians and judges have said for two centuries that a robust and wide-open debate of public issues is vital to the democratic process. The Administration’s TSP program targeted subversive political views associated with extremist ideology, which runs counter to U.S. Democracy. Although the program officially targets terrorist and terrorist sympathizers, many of the defendants claim they were targeted due to their political associations or religious views.

The Administration argues that terrorism exists in a new paradigm that merits increased surveillance in order to deter internal and external threats to national security, but the founders knew of threats to liberty. Indeed, since the creation of this country there have been laws to limit speech associated with dissident viewpoints. The TSP may have been conceptualized and rationalized as a utopian panoptic tool for ensuring national security, yet in application it was executed in a way that had the potential to create an Orwellian dystopia in the United States. If every uttered word with an “ism” attached to it is deemed to be contradictory to U.S. democracy, then the free exchange of ideas will be halted in the name of protecting American ideals.

The Terrorist Surveillance Program may also act as a regulation of communications content delivered through telephony. Citizens might assume that their telephone conversations

---

are private as long as they don’t discuss controversial topics or advocate politically unpopular ideas. This might cause some citizens to be less inclined to engage in discussions of the vital current public issues. The War on Terrorism does not so much create a new paradigmatic justification for programs such as the TSP, as it represents a new technological age that enables more sophisticated surveillance of society. Terrorism has not created a new paradigm; technology has created a new frame through which we must evaluate First Amendment protections for free expression.

So has the *Hepting* case exposed a need for change in the current law? No more than any of the other cases that came about as a result of the Administration’s acknowledgement of the Terrorist Surveillance Program. It appears that the current surveillance scandal echoes cloak-and-dagger spying of the pre-FISA era. The intent of FISA was to prevent the abuse of powers in regards to domestic spying. Although the American public might be concerned with the intentions of the Bush Administration, two key factors cast doubt on the plaintiff’s claims.

First, FISA allows for warrantless domestic surveillance if authorized by statute. If the government can show that the Authorization for Use of Military Force satisfies this requirement, then the Terrorist Surveillance Program would not violate FISA. The Supreme Court confirmed the expansive language of the AUMF in 2004, creating a precedent for how the AUMF would be viewed. In *Hamdi v. Rumsfeld*, the court ruled that the President could use “all necessary and appropriate force” in waging war and preventing enemy attacks, specifically, American citizens could be detained as enemy combatants.75 The Attorney General has argued that this establishes a precedent for the AUMF to act as a statute required to satisfy FISA.

---

Although there is judicial precedent for the administration using the AUMF as a statutory exemption to FISA, there is debate over the ruling and if Congress intended for the authorization to be used in such a manner. A Congressional Research Service report from January 2006 states that the Administration has interpreted the AUMF too broadly and that Congress had no intent of expanding the President’s war-making powers. Constitutional scholars are at odds over the administration’s interpretation of Congressional intent. Although some experts side with the Administration’s reasoning, others disagree with the loose interpretation of FISA’s statutory exemption.

AT&T customers agree to the company’s privacy policy through their continued use of provided services. The AT&T privacy policy explicitly states that the company can use and disclose customer identifiable information for the purposes of preventing physical harm to others, or investigating or preventing unlawful activities. Terrorism is defined as the use or threat of violence to intimidate or cause panic, especially as a means of affecting political conduct. Even without court orders or official government authorizations, the plaintiffs, through the privacy policy, have already agreed to allow AT&T to intercept and disclose communications. If AT&T suspected the plaintiffs of engaging in terrorism, then the “threat of violence” involved would most certainly qualify as a preventable physical harm and an unlawful activity.

This said, it would be necessary for the plaintiffs to prove that AT&T, on behalf of the government, was not specifically targeting them, but rather a large population of customers. If the individual plaintiffs were suspected of terrorism, then the government might have some basis for the surveillance. If the program were revealed to mimic Operation Shamrock’s large-scale data mining, then it would be more difficult for the government to prove it had specific evidence.

76 BLACK’S LAW DICTIONARY 1484 (7th ed. 1999).
to incriminate the plaintiffs. However, as discussed previously, disclosure of program details is unlikely because it could jeopardize endeavors to catch actual terrorist by revealing privileged information.

Even so, the implications of the Hepting case could be significant. If AT&T is found liable, then contractors could be vulnerable to lawsuits that allege their voluntary participation in illegal activities through compliance with the government. If the Bush Administration’s claim that the AUMF is a sufficient statutory exemption to FISA is upheld, it could change the nature of domestic surveillance. If all telephone communications were potentially subject to and in fact the focus of a government data-mining program, the disclosure of that information could have a potential chilling effect on the First Amendment rights of American citizens to free speech and free association.

Perhaps Michael Hayden was right in his 2002 statement that “We need to get it right.” What is especially revealing after examining current laws and the AT&T case is the need for clarification in the law. Although the Bush Administration is following the letter of the law, it might not necessarily be honoring the intent of legislators who originally designed FISA to prevent the very kind of surveillance the executive is accused of engaging in. In this way, the shifting line between security and liberty demonstrates a need to reevaluate the intelligence paradigm through a lens most appropriate in the new millennium.

**Future Remedies**

The electronic surveillance system in the United States might be improved by requiring more accountability of intelligence gathering agencies. In honoring the security v. liberty balance, and in working for better oversight, the best possible model might be an independent oversight commission that monitored surveillance related issues and reported on discrepancies in warrant execution. This type of commission could operate independent of the three branches of
government and could be staffed by intelligence officials, civil liberties activists, attorneys, congress members, judges, telecommunication executives and citizens. Even with this type of oversight, there is still the issue of how future communications will be handled. We, as a nation, are at a volatile period in our technological development. Even as the Courts and Congress struggle to determine the legality of the government and telecommunications companies collaborating under the Terrorist Surveillance Program, new technologies are gaining ground and changing the very network updated laws seek to govern.

Congress has also addressed the issue of independent oversight in its FISA Amendments Act of 2008, which has been passed by the Senate and is currently under consideration by the House. The act recommends the creation of a Commission on Warrantless Electronic Surveillance Activities, to report to Congress on all intelligence collection programs and activities inside the United States or regarding U.S. persons since the 9/11 terrorist attacks.\textsuperscript{77} Under the FISA Amendment Act, the Commission would protect national security and submit interim reports on intelligence activities.\textsuperscript{78}

Another future remedy is the reconciliation of new technologies with government needs to monitor communications in the interest of protecting national security. In 2004, Privacy International, an advocacy group for privacy rights, reported on an Federal Communications Commission ruling in response to government agencies’ filings in a proposed rulemaking on the future of Broadband Internet and Voice Over Internet Protocol regulation. The ruling applied CALEA to these new services, requiring communication carriers to build in surveillance-ready


\textsuperscript{78} Id. at § 301(b)(2).
access points for government interception. The FCC commissioners sought to provide compliance clarity to law enforcement and providers of enhanced communications services. FCC Chairman Michael Powell said that the nation is entering, “dynamic space in the evolution of Internet voice services and applications.” He said the FCC must “continually assess” how these “technologies re-shape communications,” since increasing numbers of customers are using the new offerings. He highlighted the commission’s past stance to minimally regulate the Internet, but added that it is “essential” for law enforcement to be able to access this type of communication, even if they are “information services,” under the Communications Act. Powell added that the commission’s support for law enforcement is “unwavering,” in its needs to “combat crime and terrorism and support Homeland Security.”

Commissioner Kathleen Abernathy also supported the ruling, as well as law enforcement agencies’ need for tools to “conduct surveillance in a changing technological environment.” However, Abernathy expressed concern over the rulings incompatibility with the regulation of information services under the Communications Act:

While the text and legislative history of CALEA make clear that the march of technological progress should not hamper law enforcement’s ability to conduct lawful wiretaps, the statute also explicitly exempts information services from its reach. The Commission has proposed a means of resolving this tension, but it remains to be seen whether our attempts to do so would pass judicial muster.

Commissioner Michael Copps emphasized the need for judicial approval in regards to the ruling. He said the reasoning behind the decision stretched the “statutory fabric to the point of tear,” since CALEA’s application to information services had not been tested in the courts.

---

What impact an independent surveillance commission or new telecommunications technologies will have on current electronic surveillance standards is unclear. However, in recognizing the need for updated approaches to monitoring government intelligence activities, both the Congress and the Federal Communications Commission have begun to address emerging issues that will likely be the subject of future laws and rulings.

**Future Research**

This research has established a cyclical relationship between the passage of electronic surveillance laws and time periods where there is increased concern for protecting national security. These laws, and subsequent judicial decisions upholding their legality have been hesitant to recognize the need for political dissent in the marketplace during times of national crisis. Although cases involving the constitutionality of electronic surveillance have been traditionally decided on Fourth Amendment grounds, there is a penumbra right to privacy in communication that comes from the nexus of First and Fourth Amendment constitutional rights. This research reveals the link—between traditional Fourth Amendment protections against search and seizure and the First Amendment’s protections for free speech and association—that is critical in evaluating current and future court decisions involving government surveillance programs.

Recent technological advancements in the telecommunications industry have created a reliance on phone communication as a tool for free political expression in the marketplace of ideas. Government restriction on private communications of this nature could create a chilling effect on free expression essential to the democratic process. The research presented here is unique in that it explores this chilling effect by applying Lasswell’s theories of a security elite and Emerson’s values in protecting free speech. Both Lasswell and Emerson’s theories are traditionally applied in political circumstances, but have not—until now—been used to evaluate
electronic surveillance. The legality of electronic surveillance—when evaluated against the backdrop of Lasswell and Emerson’s theories—reveals a shifting balance between the need to protect civil liberties and the need to protect national security. The current balance is weighted more towards protecting national security during the War on Terror.

Finally, contemporary warrantless surveillance programs—leaning more towards protecting national security—were analyzed to explore their chilling effect on speech in the marketplace. Although court cases filed in response to these programs were not substantially filed or decided on these grounds, the chilling effect discussed in this research could be seen as a prior restraint on speech, demanding higher standards of judicial scrutiny under First Amendment protections.

The issues explored in this research and analysis make no final conclusions due to the pending status of the contemporary cases reviewed. Technological advancements in the telecommunications network have resulted in a situation where government can engage in intelligence gathering activities that eclipse those envisioned by Congress in its drafting of the current surveillance laws. The Patriot Act allowed the use of pen registers to address emerging technological capabilities, but the convergence of wire, wireless and fiber optic communication lines present new challenges for federal agents seeking to track moving targets. Future research is needed to study how Congress will amend current electronic surveillance law to meet these changing needs.

Additionally, future research is needed to determine the legality of the ongoing government surveillance strategies. Although the Terrorist Surveillance Program was brought under judicial oversight and Attorney General Gonzales said it would not be reauthorized, other enhanced intelligence gathering tools remain. The PATRIOT Act barred recipients of National
Security Letters from disclosing the fact that they had received a letter if the disclosure would endanger national security, human life, diplomatic relations or ongoing intelligence investigations. Although the original PATRIOT Act did not require judicial review of national security letters, the current reauthorization of the act does provide for judicial review by the FISA Court. Further research is needed to determine if the new authorization process—even though it provides judicial authorization for National Security Letters—might act as a prior government restraint on free speech under the First Amendment.

Additional research is needed to investigate the feasibility of a holistic judicial approach to constitutional protections for citizens who are the targets of electronic surveillance. The Supreme Court has acknowledged a penumbra of unnamed rights emanating from the First, Third, Fourth and Fifth Amendments of the Bill of Rights. One of these unnamed rights—individual privacy rights—was recognized by the Court in the 1965 *Griswold* case involving a state law banning contraceptives. Although this “penumbra” right for privacy was recognized by the Court for its applicability to marital privacy, it has not been fully developed as protection against the electronic surveillance of communication contents. Future research is needed to determine if the Court is willing to extend the First Amendment’s right of association, the Fourth Amendment’s guarantee against unreasonable search and seizure and the Fifth Amendment’s privilege against self incrimination to protect the privacy of citizens’ communications.

Extending First Amendment protections to electronic surveillance would also create a higher standard of review for government intelligence gathering activities that targeted political activities of citizens. Historically, the Court has decided electronic surveillance cases on plaintiff’s claims alleging a violation of the Fourth Amendment’s guarantee against unreasonable

---

search and seizure. If the government can show that the surveillance was properly authorized through judicial review, the Court often dismisses the plaintiff’s claims, as the government has established that it honored the constitutional protection by obtaining a warrant. However, if the Court were to evaluate a plaintiff’s claim of illegal electronic surveillance on First Amendment grounds, there would be a higher standard of review, as the Court would need to determine that the Congressional statutes governing electronic surveillance had created no prior restraint on citizen speech. The contemporary cases discussed begin to hint at this shift in constitutional philosophy, but a full analysis of the final case holdings will be needed before the feasibility of this type of judicial review can be determined.
LIST OF REFERENCES

Statutes, Codes, Regulations, and Constitutions


Certain intelligence officials: consultation and concurrence regarding appointments; evaluation of performance, 10 U.S.C § 201 (2000).


THE DECLARATION OF INDEPENDENCE (U.S. 1776).


U.S. CONST. prmb1.

U.S. CONST. art. II, § 2.

U.S. CONST. amend. I.
U.S. CONST. amend. IV.
U.S. CONST. amend. V
U.S. CONST. amend. XIV


Cases


Bridges v. California, 314 U.S. 252 (1941).


Clayton/Gaw v. AT&T, No. 06-cv-4177 (W.D. Mo. 2006).


Conner v. AT&T Corp., No. 1:06-632 (E.D. Cal. 2006).


Dolberg v. AT&T Corp., No. 9:06-78 (D. Mont. 2006).


Ex parte Jackson, 96 U.S. 727 (1878).


Frohwerk v. United States, 249 U.S. 204 (1919).


Harris v. United States, 331 U.S. 145 (1947) (Frankfurter, J., dissenting).


Hester v. United States, 265 U.S. 57 (1924).


Kasza v. Browner, 133 F.3d 1159 (9th Cir. 1998).


Mahoney v. AT&T Commc’ns, Inc., No. 1:06-223 (D.R.I. 2006).


Mink v. AT&T Commc’ns of the Sw., Inc., No. 4:06-cv-01113 (E.D. Mo. 2006).


Potter v. BellSouth Corp., No. 3:06-469 (M.D. Tenn. 2006).


Schwarz v. AT&T Corp., No. 1:06-2680 (N. D. Cal. 2006).


Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920).

Souder v. AT&T Corp., No. 3:06-1058 (S.D. Cal. 2006).


Supreme Court Order List (Feb. 19, 2008) available at 


Terkel v. AT&T Inc., No. 1:06-2837 (N.D. Cal. 2006).


Times-Mirror Co. v. Superior Court, 310 U.S. 623 (1941).


United States v. Brown, 484 F.2d 418 (5th Cir. 1973).


United States v. Gaw, No. 06-1-cv-1132 (E.D. Mo. 2006).


United States v. Lee, 193 F.2d 306, 317 (2d Cir. 1951) (dissenting opinion).


United States v. Rabner, No. 06-cv-2683 (D.N.J. 2006).


United States v. Truong, 629 F.2d 908 (4th Cir. 1980).


**Legislative Materials**

1 ANNALS OF CONG. 439 (Gales ed. 1834).

114 CONG. REC. 14751 (1968).


190 Parl. Deb. (3d ser.) 1517 (1868).


SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, 94TH CONG., FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES (“CHURCH COMMITTEE FINAL REPORT”) (1976).


Administrative and Executive Materials

Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11, 2 PUB. PAPERS 1140 (Sept. 20, 2001).


President’s Radio Address, 41 WEEKLY COMP. PRES. DOC. 1880 (Dec. 17, 2005).


Military Intelligence Section 8 (MI-8).


NATIONAL SECURITY AGENCY, NSA/CSS MANUAL 22-1, at 7 (1986).


Secondary Sources


ERIK BARNOUW, A TOWER IN BABEL (1966).


ISAIAH BERLIN, LIBERTY (2002).


BLACK’S LAW DICTIONARY (7th ed. 1999).


William J. Brennan, Jr., The Quest to Develop a Jurisprudence of Civil Liberties in Times of Security Crises, Speech at the Law School of Hebrew University, Jerusalem, Israel, at 1 (Dec. 22, 1987).


Exodus 20:4-5.

THE FEDERALIST NO. 2 (John Jay).


Heath H. Galloway, Don’t Forget What We’re Fighting For: Will the Fourth Amendment Be A Casualty of the War on Terror, 59 WASH. & LEE L. REV. 921 (2002).


HAROLD LASSWELL, NATIONAL SECURITY AND INDIVIDUAL FREEDOM 141-42 (1950).


Declan McCullagh & Anne Broache, Some companies helped the NSA, but which? CNET News.com, Feb. 6, 2006 (last visited June 14, 2008).


ALEXANDER MEIKLEJOHN, POLITICAL FREEDOM (1960).


JOHN MILTON, AREOPAGITICA 21 (Everyman's Library 1927) (1644).


Lawrence D. Sloan, Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation, 50 DUKE L.J. 1467 (2001).


*Samuel Stouffer, Communism, Conformity, and Civil Liberties* 89-90 (1955).


BIOGRAPHICAL SKETCH

Sunny Skye Hughes earned her doctorate from the College of Journalism and Communications at the University of Florida in 2008. Hughes earned her bachelor’s degree in 1997 from Texas A&M University in journalism with a minor in political science. She completed her master’s degree in telecommunications at the University of Florida in 2005.

She is currently an associate professor of broadcast journalism at the University of Maine in Orono, where she teaches mass media writing, television news reporting and production. Her research interests include the First Amendment implications of electronic surveillance, open government and press-government relations. In the past, Hughes has taught Introduction to Telecommunications, Introduction to Public Speaking, Interpersonal Communication, and Modes of Inquiry. Hughes has also done legal research for the Marion Brechner Citizen Access Project at the University of Florida in Gainesville.

In Texas, Hughes worked as a reporter in public television, traffic director in public radio, produced a community affairs show, *Brazos Arts*, and was the assistant development director for KAMU-TV & FM. She also worked as a news producer for KOAT-TV in Albuquerque and WUFT-TV at the University of Florida.

Hughes produced the *Government in the Sunshine* video for the Brechner Center for Freedom of Information in 2004. She has presented research at conferences organized by the Broadcast Education Association (BEA) and the American Educators in Journalism and Mass Communication (AEJMC), as well as the National Communication Association (NCA).