2011

Defining the contours of the national surveillance state: analyzing the development of electronic surveillance

Brett Rubio
Western Washington University

DEFINING THE CONTOURS OF THE NATIONAL SURVEILLANCE STATE: ANALYZING THE DEVELOPMENT OF ELECTRONIC SURVEILLANCE

By

Brett Rubio, J.D.

Accepted in Partial Completion
of the Requirements for the Degree
Master of Arts

Moheb A. Ghali, Dean of the Graduate School

ADVISORY COMMITTEE

Chair, Dr. Paul Chen

Dr. Sara Weir

Dr. Johann Neem

MASTER'S THESIS

In presenting this thesis in partial fulfillment of the requirements for a master's degree at Western Washington University, I agree the Library may make copies freely available for inspection.

Library users are granted permission for individual, non-commercial reproduction of this work for educational research purposes only.

I represent and warrant this is my original work, and does not infringe or violate any rights of others. I warrant that I have obtained written permissions from the owner of any third party copyrighted material included in these files.

I acknowledge that I retain ownership rights to the copyright of this work, including but not limited to the right to use all or part of this work in future works, such as articles or books.

Any copying or publication of this thesis for commercial purposes, or for financial gain, is not allowed without my written permission.

Brett Rubio, J.D.
November 1, 2011

DEFINING THE CONTOURS OF THE NATIONAL SURVEILLANCE STATE: ANALYZING THE DEVELOPMENT OF ELECTRONIC SURVEILLANCE

A Thesis
Presented to
The Faculty of
Western Washington University

In Partial Fulfillment
Of the Requirements for the Degree
Master of Arts

By

Brett Rubio, J.D.
November 2011

Abstract

The theory of a National Surveillance State, as provided by Balkin and Levinson, provides a broad framework for understanding the increased use and implications of electronic surveillance by the United States government. This thesis traces the development of electronic surveillance in the United States and evaluates how certain provisions of the Patriot Act have reduced privacy rights and have empowered the Executive branch with greater authority. As established by the theory of a National Surveillance State, the need for electronic surveillance is evident, yet it should be conducted within the context of constitutional protections of individual rights and political checks and balances.

Acknowledgments

While on the title page of this thesis, my name appears as sole author, this study would not have been possible without the continuous help and support of many others. Words seem insufficient to express my gratitude and there are many people to thank.

I could not have done this on my own and my thesis is dedicated to the following wonderful individuals:

Dr. Paul Chen: My advisor and mentor who went through many, many a draft helping me to solidify my arguments, and through whose careful tutelage I finally arrived to my "Final" draft. Thank you for your advice and insistence on rigor.

Sheila and Bradley: My wife and son who supported and encouraged me throughout the thesis process. They provided me with the love and confidence I needed on the days I never thought I'd get done. Thank you for your love and encouragement.

Dr. Vernon Damani Johnson: My graduate school advisor and mentor who willingly provided me a much needed sounding board and lead me to complete all my graduate school requirements in an enjoyable manner. Thank you for your support and sense of humor.

Dr. Sara Weir and Dr. Johann Neem: My committee, who provided me with valuable suggestions as I completed this project. Thank you for your guidance.

My colleagues and friends in the Political Science department: Those friends and officemates, who forced me to take occasional breaks, and who repeatedly reminded me that I could and *would* finish. Thank you for your help and friendship.

Table of Contents

Figures

Appendices

"[T]he tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping."

Justice Louis Brandeis
Dissenting opinion in
Olmstead v. United States
(277 U.S. 438, 1928, p. 476)

Introduction

The tragedy that beset the United States on September 11, 2001 prompted the federal government to take immediate measures towards preventing similar terrorist attacks in the future. Legislators expressed frustration with the failures of intelligence agencies and law enforcement to piece together clues of the impending attacks.[1] Without any hearings or floor debates, Congress passed the USA PATRIOT Act (Patriot Act)[2] less than two months after the September 11 attacks. The Patriot Act amended several existing bills of federal legislation and notably expanded law enforcement authority to conduct electronic surveillance by blurring the long standing line between domestic law enforcement surveillance and foreign intelligence gathering. The distinction is often referred to as the "wall." The constitutional significance is that the former comes with civil liberties protection while the latter has almost no constitutional protection.

---

[1] *See* Michael T. McCarthy, *Recent Developments-U.S.A. PATRIOT Act*, HARV. J. ON LEGIS. 39: 435, 437-38 (noting that prior to September 11, the Central Intelligence Agency had intelligence on two of the hijackers, identifying them as suspected terrorists, but the Agency failed to share that information with the Federal Bureau of Investigation or Immigration and Naturalization Service in time for them to prevent the hijackers from entering the country).

[2] The Act is entitled: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 [hereinafter Patriot Act].

The attacks of September 11 along with the advancement of electronic surveillance technology contributed to what law professors Jack Balkin and Sanford Levinson call a National Surveillance State. "In the National Surveillance State, the government uses surveillance, data collection, collation, and analysis to identify problems, head off potential threats, govern populations, and deliver valuable social services. As a theory of governing, the existence of the National Surveillance State poses several constitutional concerns to our system of government."[3] These concerns include the degradation of electronic privacy for its citizens, the blurring of law enforcement and intelligence practices, and the disruption of checks and balances through the expansion of the Executive Branch.[4]

Critical Problem

It is not the purpose of this thesis to laud or condemn the Patriot Act. Instead, it is my intent to examine the evolution of electronic surveillance and to identify trends that may have broader policy implications. Professors Balkin and Levinson propose that a creation and rise of a "National Surveillance State" occurred as a result of the historical increase in government surveillance power, namely through the passing of the Foreign Intelligence Surveillance Act of 1978 and its subsequent amendments. But after the September 11 terrorist attacks, an opportunity arose to pass legislation that would again increase governmental electronic surveillance through the Patriot Act. Did the creation

[3] Jack M. Balkin and Sanford V. Levinson. *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, FORDHAM L. REV. 75: 489. p. 521.
[4] *Id.*

of the "National Surveillance State" make it possible to enact the Patriot Act? Will the Judicial Branch eventually approve these changes through constitutional doctrine, as this theory of government proposes? Or is there an alternate explanation to the National Surveillance State?

With this in mind, I provide an in-depth analysis of the development of electronic surveillance in order to argue that while government is becoming more efficient in collecting information on its citizens, potentially justifying the conclusion that a National Surveillance State exists, the Judicial and Legislative Branches historically protected citizens from this type of governmental intrusion.

Defining Electronic Surveillance

The objective of electronic surveillance when used in law enforcement is to gather evidence of a crime or to accumulate intelligence about suspected criminal activity. Electronic Surveillance is described as the observing or listening to persons, places, or activities, usually in a secretive or unobtrusive manner, with the aid of electronic devices such as cameras, microphones, tape recorders, or wiretaps.

Historically, three types of electronic surveillance are most prevalent: wiretapping, bugging, and videotaping. Wiretapping intercepts telephone calls and telegraph messages by physically penetrating the wire circuitry. Someone must actually "tap" into telephone or telegraph wires to accomplish this type of surveillance. Bugging is accomplished without the aid of telephone wires, usually by placing a small microphone or other listening device in one location to transmit conversations to a nearby

receiver and recorder. Video surveillance is performed by conspicuous or hidden cameras that transmit and record visual images that may be watched simultaneously or reviewed later on tape.

All three common forms of electronic surveillance serve several purposes: (1) enhancement of security for persons and property; (2) detection and prevention of criminal, wrongful, or impermissible activity; and (3) interception, protection, or appropriation of valuable, useful, scandalous, embarrassing, and discrediting information. The law attempts to strike a balance between the need for electronic surveillance, by law enforcement and intelligence gathering agents, and the privacy interests of those affected either criminals or unintentionally targeted citizens. This balance is often derived by courts' interpretation of the Fourth Amendment to the Constitution.

The Difference Between Law Enforcement and Foreign Intelligence

Traditionally, participants in the intelligence arena use information to gauge foreign capabilities and intentions while members of law enforcement organizations collect information to support domestic prosecution. The Fourth Amendment to the Constitution limits surveillance of Americans, and regulations and directives limit distribution of foreign intelligence to domestic law enforcement. The intelligence community focuses beyond the borders of the United States and on the future—assessing foreign trends and actions. Intelligence community analysts evaluate what they learn, interpret the importance of the information, and determine who should be informed.

Law enforcement, on the other hand, focuses on building a legal case related to a crime that already has been committed. A case is carefully constructed based on admissible evidence and is handled in a prescribed manner. For example, the rules associated with evidence chain-of-custody are designed to protect the integrity of information and reduce the pollution of evidence as much as possible. A set of procedures is followed precisely to ensure the case will be successfully prosecuted.

The Fourth Amendment and Electronic Privacy

The Fourth Amendment of the Constitution provides the foundation for limiting the government's role in collecting domestic surveillance. It protects against "unreasonable searches and seizures" and requires that warrants be issued only upon "probable cause."[5] The Fourth Amendment expresses the Framers of the Constitution wish to keep private homes free from government invasion:

> 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.[6]

The Framers crafted the Fourth Amendment mindful of the potential abuse of general warrants and therefore required specificity for warrants to search and seize. Over one hundred and seventy years later, the United States Supreme Court would require that same specificity in electronic invasions of privacy. Prominent cases regarding the use of

[5] U.S. CONST. amend. IV.
[6] *Id.*

electronic surveillance and discussed in this thesis include: *Olmstead v. U.S.*, *Berger v. N.Y.*, *Katz v. U.S.*, *U.S. v. U.S. District Court*, *U.S. v. Truong Dinh*, *Kyllo v. U.S.*, and *In Re Sealed Case*. Equally important are the Acts of Congress that sought to address the growing concerns over the use of governmental electronic surveillance; These Acts include: *The Communications Act of 1934*, *Title III of the Omnibus Crime Control and Safe Streets Act of 1968*, *The Foreign Intelligence Surveillance Act*, *The Electronic Communications Privacy Act*, and *The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*.

In summary, "the overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[7]

Recent developments in technology allow for the quick or instant communication on business, personal, or civic matters. These changes transformed our expectations of privacy; and we now expect privacy in many of our methods of communication. For instance, many people expect some level of privacy in the daily use of telephone fax machines and electronic mail.[8] In many ways, individual privacy is more important today because society has more methods to communicate personal and sensitive conversations.

In response to these developments, laws have created several protections to communicate privately, while at the same time stopping short of creating an absolute right to privacy in all communication. In general, we have allowed police to employ

---

[7] Schmerber v. California, 384 U.S. 757, 767 (1966); *see also* Illinois v. McArthur, 531 U.S. 326, 330 (2001) (stating that the Fourth Amendment was "designed to control conduct of law enforcement officers that may significantly intrude upon privacy interests").

[8] *Id.*

wiretapping in criminal investigations, and intelligence agencies to intercept foreign, and occasionally domestic, communications on a grand scale.[9] While the government regards these activities as necessary to provide security, many concerned citizens have a different perception of electronic surveillance. The emergence of wiretapping capabilities, especially since the enactment of Patriot Act, has been seen by many citizens and scholars as instruments that can easily be misused by the government.

Literature Review

In an effort to understand whether electronic surveillance legislation, such as the Patriot Act, and Supreme Court decisions facilitated the expansion of a National Surveillance State, there are a variety of sources to consider. The first are Supreme Court case decisions on electronic surveillance, which serve as primary sources. Next, I review select Congressional legislation on electronic surveillance since 1928. Finally, I look at secondary sources such as literature on electronic surveillance, drawing largely from legal and political science journals.

Supreme Court Cases

It is necessary to examine Supreme Court cases relevant to electronic surveillance, as it helps to identify general trends that developed at different points in history. A primary example is *Olmstead v. United States (1929). Olmstead* is significant because it was the first time the Supreme Court addressed electronic surveillance when

[9] *Id.*

the government wiretapped private telephone conversations without judicial approval. In a 5 to 4 decision, the court held that no constitutional violations occurred because there was no "actual physical invasion" into the conversation. *Olmstead* was the first of many court cases on electronic surveillance. As electronic surveillance technology evolved, the Supreme Court would grapple with variations of the issues presented in *Olmstead.* Not until 1967, in *Katz v. United States*, would the court overturn *Olmstead.*

Analyzing the series of Supreme Court cases on electronic surveillance is necessary to this study because it provides an in-depth understanding of how the Judicial Branch responded to the development of technology in this field. These cases provide the "Constitutional Dialogue" on electronic surveillance through the process of judicial review.

Congressional Legislation

An example of another body of primary sources are Acts of Congress such as the *Omnibus Crime Control and Safe Street Act of 1968* (commonly referred to as 'Title III'), the *Foreign Intelligence Surveillance Act of 1978* (referred to as FISA), and *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (referred to as Patriot Act).

These laws provide the legal requirement by which the Executive Branch may proceed in conducting electronic surveillance. Many of these types of laws are enacted discretionary as a result of "Policy Windows"[10] influenced by events, such as the terrorist

[10] Frank R. Baumgartner & Bryan D. Jones, *Agendas and Instability in American Politics*, Univ. of Chicago (1993).

attacks of September 11. At other times, these laws are enacted in response to the constitutional dialogue presented through judicial review. Examining these laws is germane to this study because they provide a clear explanation of Congressional intent.

Law and Political Science Journals

There is a plethora of scholarly articles on the development of governmental electronic surveillance, privacy, and the Patriot Act. Many of these articles are concerned with the possible legal ramifications of the Patriot Act. Most of these essays explore the risks to individual electronic privacy, especially in banks, business, and libraries. The majority of these articles normally lay out a brief history of decisive cases and legislation before stating the author's position on the possible threat to electronic privacy. This literature is useful in providing legal background on the development of electronic surveillance and perspective on this topic. However, most of these articles do not speak directly on broader policy topics, such as the theory of a National Surveillance State, which this study seeks to do.

The most noteworthy articles on the theory of a National Surveillance State come from three essays. Jack Balkin and Sanford Levinson first describe their theory of a National Surveillance State in their article *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State* (2006). They propose a theory of a National Surveillance State that is established as a result of political conditions and the expansion of technology. The political conditions are primarily a result of the Legislative and Executive branches forcing unconstitutional changes in governance, through collection of information, and ultimately the Judicial Branch, while initially

resisting, cooperating with these changes. Lastly, through the force of legislation and Executive responses to warfare, the government is set on increasing its information collecting on potential suspects thus justifying and expanding its powers of surveillance. This theory of a National Surveillance State serves as the framework to analyze the expansion of governmental electronic surveillance.

In a subsequent article, Jack Balkin in an essay entitled *The Constitution in the National Surveillance State*, builds on the National Surveillance State theory by arguing that the private sector will gain from this form of governance. Balkin warns us to the possibility that government will attempt to absolve itself from major legal restrictions by investing in the private sector in order to collect information on its citizens. Balkin claims that resisting this political condition would require the enactment of "super-statutes" because the courts would be unable to enforce Fourth Amendment protections on privacy. These statutes would regulate the collection of information in three important ways: 1. They would restrict the type of information that the government may collect, 2. They would create a code of conduct for the collection of information by private companies, and most importantly, 3. They would create a series of oversight mechanisms for executive bureaucracies. Here again, Balkin provides a useful context to analyze whether the development of governmental electronic surveillance has contributed to this theory of governance.

This National Surveillance State caught the attention of a legal scholar at George Washington University, Professor Orin Kerr, a leading scholar in the field of Criminal Law and Procedure, who wrote a law review essay responding to this theory of governance. In *The National Surveillance State: A Response to Balkin*, Kerr claims that

making changes to existing laws is the best method in addressing technology concerns pertaining to electronic surveillance. He states that these changes should address the advances in technology in order to maintain traditional constitutional protections. He argues that addressing the technological challenges in this manner is far more useful that proposing a theory of government hell-bent on collecting as much information as it can on its citizens. As an alternative explanation to the National Surveillance State, Kerr describes these technological challenges as a "shift to computerization" whereby the use of computers by the government allowed for a more efficient method of collecting and analyzing information from citizens. Kerr's counterpoint is directly relevant in analyzing whether the development of governmental electronic surveillance contributes to either of these theories.

A review of these literatures pertaining to the expansion of electronic surveillance reveals a great deal of information, but little on how it relates to the theory of a National Surveillance State. While there has been significant research on the legal ramifications of the evolution of electronic surveillance, very few scholars looked at how it might relate to a broader theory of governance.

Methodology

In carrying out this study of the evolution of electronic surveillance, by using the theory of a National Surveillance State as a framework, I conduct a broad inductive analysis using the following steps. First, I analyze four key provisions in the Patriot Act and show how they amended/changed the existing law on electronic surveillance.

Second, I survey the historical development of governmental electronic surveillance to identify emerging patterns and to determine how the Judicial and Legislative branches responded to this development. This includes examining key Supreme Court decisions as well as acts of Congress.

Last, I will combine the inductive descriptions previously mentioned to show the relationship between the expansion of electronic surveillance and the courts' response in protecting traditional constitutional protections. Using the broad inductive analysis described above, I will provide a clear description demonstrating that while the government is increasing its collection of electronic information on its citizens, as stated in the National Surveillance State, the courts are cautiously limiting those powers in order to preserve traditional constitutional protections to privacy.

Outline of Thesis

In chapter one, I provide a comprehensive analysis of Balkin and Levinson's theory of a National Surveillance State, and how the private sector may gain from this theory of governance. I then provide an alternative view to this theory by describing Kerr's response that what is taking place is instead a "shift to computerization." I then explain/discuss how the Patriot Act may contribute to the theory of a National Surveillance State. In chapter two, I analyze how amendments to FISA, and other changes to electronic surveillance through the Patriot Act, have changed individual electronic privacy. Specifically, I review four key sections of the Patriot Act: Allowing for Roving Wiretaps, the Seizure of Voice Mail, Pen Registers and Trap-and-Trace

Devices, and the change of purpose of foreign intelligence gathering from "primary" to "significant."

In chapter three, I define electronic surveillance and review how the Fourth Amendment historically offered individual electronic privacy protection. Further, I analyze the legal framework of domestic electronic surveillance and discuss legislation that address these concerns such as the enactment of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Foreign Intelligence Surveillance Act (FISA). I then present a final conclusion, in chapter five, about what this study has revealed about the development of electronic surveillance by using the framework of a National Surveillance State theory. Lastly, I conclude by offering further research questions that will encourage additional research in this field.

Contribution to the Field

Numerous essays on electronic surveillance and the Patriot Act are found in law and policy journals. Many of them cover possible legal ramifications, often in specific venues, such as banking and private business. Other essays explore the Patriot Act and FISA purely in the context of the legal system, while some concern themselves with policy implications. There is a significant lack of scholarly analysis, however, in essays that study these areas collectively, and even fewer that discuss electronic surveillance from the context of a theory of governance: the National Surveillance State. This thesis aims to provide a complete and coherent understanding of the state of electronic

surveillance in the context of the National Surveillance State theory, thereby contributing to this field of study.

Chapter One: Examination of the National Surveillance State

This chapter examines the theory and the development of a National Surveillance State, as proposed by Jack Balkin and Sanford Levinson, and the type of threats that are created by this theory of governance. I argue that while the threats described by Balkin and Levinson are real, they are of less concern than they propose based on the historical analysis that I conduct in chapter three.

This chapter will also discuss possible measures that can be applied to contain these threats and present how the private sector is likely to become involved with this theory of government. I will also set forth an alternative view to the National Surveillance State as described by Orin Kerr. Finally, I give a brief description of the National Surveillance State in relation to the USA Patriot Act in order to explore the belief that this type of legislation facilitated the advancement of this state.

Development of the National Surveillance State

Law professors, Jack Balkin and Sanford Levinson, describe that certain political conditions have led to what they call a National Surveillance State. These conditions include the government's need to gather information on individuals and groups suspected of posing a threat to national security. In the National Surveillance State, "the government uses surveillance, data collection, collation, and analysis to identify

problems, head off potential threats, govern populations, and deliver valuable social services."[11]

Balkin and Levinson argue that the development of information technology is the primary engine of the National Surveillance State because it facilitates the efficient collection of information by the government. They argue that as technologies "become more powerful, both governments and private parties will seek to use them"[12] to better understand human behavior and prevent terrorist acts. The expansion in the use of technology is exemplified by the government's investments in high-speed computers. The newly developed technology can process complex mathematical algorithms to "recognize" patterns of speech, telephone contact information, e-mail messages, and Internet traffic that might indicate possible terrorist or criminal activity.[13] The state can utilize these technologies for collecting foreign intelligence and preventing attacks on the information infrastructure.[14]

Legislative responses to terrorism, such as the *Patriot Act*, the *Electronic Communication Privacy Act of 1934*, *Omnibus Crime Control and Safe Streets Act of 1968*, and the *Foreign Intelligence Surveillance Act of 1978*, play a pivotal role in advancing a National Surveillance State, argue Balkin and Levinson because ultimately they help expand governmental surveillance. They also maintain that the creation of a National Surveillance State represents the "major constitutional development of our

[11] Jack M. Balkin, *The Constitution in the National Surveillance State* MINN.L. REV. 1 (2008) 93:3.
[12] *Id.*
[13] Jack M. Balkin and Sanford V. Levinson. *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, FORDHAM LAW REVIEW 75: 489. p. 521.
[14] *Id.*

era"[15]because the development of this state is necessary in order for government to respond to the ever changing and "particular needs of warfare, foreign policy, and domestic law enforcement in the twenty-first century."[16] They cite as examples the new digital communication technologies that allow terrorist organizations to hide their identities, encrypt their communications, transfer funds and resources, and gather allies in many different places around the world.[17] As such they maintain that government has increased its use of surveillance technology as terrorists have increasingly taken advantage of these communication technologies to hide their activities.

Balkin and Levinson argue that if the Executive branch is able to conduct surveillance on its Citizens without sufficient judicial review and legislation, it would lead to an unchecked authority of the Executive Branch. The end result, according to Balkin and Levinson, is that this system of governance is likely to diminish our system of checks and balances, potentially making the Executive branch the most powerful political arm of government. Balkin and Levinson declare that courts may initially resist some of these security changes, but in the long run, they cooperate with them, shape their contours, and legitimate them through the development of constitutional doctrine.[18]

---

[15] Jack M. Balkin and Sanford V. Levinson. *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, FORDHAM L. REV. 75: 489.
[16] *Id.*
[17] Jack M. Balkin and Sanford V. Levinson. *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, FORDHAM L. REV. 75: 489. p. 521.
[18] *Id.*

Private Sector Involvement in the National Surveillance State

Similar to the partnership between the U.S. government and in the private defense industry, which acts to further the placement of weapons systems to project power world-wide, the National Surveillance State will require the partnership of the private sector to conduct surveillance.[19] According to Balkin, government and businesses are co-developing surveillance, data-mining and information analysis. Moreover, because there are many possible methods of Internet attacks, this requires governments, corporations and private parties to work together to protect network security and prevent threats before they occur.[20] To this end, the government and private sector will be interested in amassing large amounts of information from individuals and groups to determine if useful information can be derived, such as determining if a terrorist threat exists.

> "Government's most important technique of control is no longer watching or threatening watching. It is analyzing and drawing connections between data. Much public and private surveillance occurs without any knowledge that one is watched. More to the point, data mining technologies allow the state and business enterprises to record perfectly innocent behavior that no one is particularly ashamed of and draw surprisingly powerful inferences about people's behavior, beliefs, and attitudes."[21]

Because the Constitution is limited in reaching private parties, the government has an increased incentive to rely on private enterprise to collect and generate information.[22]

---

[19] Jack M. Balkin, *The Constitution in the National Surveillance State,* MINN. L. REV. 93: 1 (2008).
[20] *Id.*
[21] *Id.* at 9.
[22] Christopher Slobogan, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 320-21 (2007).

Threats Created by the National Surveillance State

Under the National Surveillance State, changes to electronic surveillance laws, such as the ones made by the Patriot Act, create several constitutional concerns about our system of government. According to Balkin and Levinson, there are two primary and distinct dangers.

The first danger is that the Executive Branch's power to conduct war and combat terrorism will displace the area previously assumed to fall within the criminal justice system.[23] This is especially true in matters of electronic surveillance, where it can be difficult to distinguish between domestic and foreign communications. If a suspected terrorist phone call is made from a foreign country to a U.S. citizen, the government can argue that the communication is foreign and is therefore within the jurisdiction of the Executive branch's war powers, versus traditional domestic law enforcement jurisdiction. Therefore, there is a lure for the Executive Branch to treat these types of communications as matters of war and national security, rather than matters of criminal justice. The latter is not subject to the same judicial oversight used in domestic law enforcement.

The risk presented by this situation is that the criminal justice system operates with a series of traditional civil liberties protections that constrain the state, while there is less civil liberty protections required for foreign communications. Allowing the government to collect information on citizens, with less constitutional protections, would

[23] Jack M. Balkin and Sanford V. Levinson. *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, FORDHAM L. REV. 75: 489. p. 521.

increase the power of the Executive branch and disrupt the checks and balances among the political branches.

The second danger is that the traditional criminal justice system will become increasingly like the national security judicial system. The risk here is that law enforcement agencies will be tempted to move from investigation and arrests after crimes occur, to surveillance, prevention, and interceptions before crimes occur.[24] After all, if we can keep our citizens safe from Al Qaeda using the most advanced information technologies, why not use those technologies to protect our citizens from ordinary crimes?[25] This outcome is likely to change the criminal justice system by limiting, key legal protections, such as judicial oversight, leading to the disruption of checks and balances.

The risk to checks and balances can lead to the courts yielding their judicial review authority to law enforcement. Balkin and Levinson argue that while it is not likely that judges will willingly yield this authority at first, over the long run they cooperate with Executive Branch decisions. They reason that roving wiretaps, which will be discussed at length later, serve as a fitting example. The judicial oversight of wiretapping phones through separate wiretap warrants has been effectively removed in favor of expediency. Roving wiretaps now permit a single wiretap warrant to cover a suspect, instead of a single telephone. This result has diminished a critical judicial step when law enforcement officers request wiretaps for electronic surveillance.

[24] *Id.*
[25] *Id.*

According to Balkin and Levinson, Congress must pass new "super-statutes" to regulate the collection, collation, purchase and analysis of data. These new super-statutes would have three basic features. First, they would restrict the kinds of data governments may collect, collate and use against people. They would strengthen the very limited protections of e-mail and digital business records, and rein in how the government purchases and uses data collected by private parties. Second, the new super-statutes would create a code of proper conduct for private companies who collect, analyze, and sell personal information. Third they would create a series of oversight mechanisms for executive bureaucracies that collect, purchase, process, and use information.[26]

Finally, technological oversight will probably be an indispensable supplement to legal procedures. They argue that we should construct surveillance architectures so that government surveillance is regularly recorded and available for audit by ombudsmen and executive branch inspectors. Records of surveillance can, in turn, be subjected to data analysis and pattern matching to discover any unusual behavior that suggests abuse of procedures. These technological audits can automate part of the process of oversight; they can assist ombudsmen, executive officials, Congress, and the courts in ensuring that surveillance practices stay within legal bounds. [27]

---

[26] *Id.*

[27] Jack M. Balkin, *The Constitution in the National Surveillance State*, MINN. L. REV. 93: 1 (2008).

Balkin and Levinson's concept of a National Surveillance State, created by the development of new technologies and political conditions, does not satisfy Professor Orin Kerr's view that a new form of governance exists. Kerr's response is that Balkin and Levinson "Leave us with a question: will the National Surveillance State be an "authoritarian information state" that controls us, or a "democratic information state" that we citizens control?"[28]

Kerr argues that our form of government remains very much the same but with a new playing field. The government's goals have not changed, Kerr states, just as before, the public wants terrorists caught and criminals prosecuted. But that old job must now be done in a new way. Kerr's explains that an alternate explanation to a "National Surveillance State" is instead a natural "shift to computerization", whereby computers are taking over surveillance and non-surveillance functions that were previously managed by humans. Therefore, laws must be created so that government can constitutionally use these devices and the information processed and analyzed so that intelligence and law enforcement officers can use it and understand what is happening. Kerr explains that "...the old job must now be done in a new way."[29] This new way allows computers and electronic surveillance to do the job that was once left for humans to do.

Ultimately, he believes that the best method to address privacy concerns, such as government use of electronic surveillance, is to create laws that address changes in

[28] Jack M. Balkin, *The Constitution in the National Surveillance State*, MINN. L. REV. 93: 1 (2008).
[29] *Id.*

technology rather than perpetuating the idea that a new concept of governing is created to secretly (and unlawfully) conduct surveillance on its citizens.

Where Balkin and Levinson see a governance problem that looks to traditional solutions such as judicial review and legislative oversight, Kerr sees a technology issue instead. Unlike the super-statutes that Balkin and Levinson propose, Kerr believes that addressing these technological issues can be accomplished through new legislation that address these concerns and thereby garners a broader political audience. Framing the issue as a technology problem enables reformers to make an institutionally conservative argument for change: if technology has changed, the law should change with it to restore the status quo ante. Further, it focuses attention on technical issues that can draw broad agreement rather than ideological claims that tend to trigger disagreement and distrust.[30]

In Kerr's view, it will take time for the legal system to appreciate this shift to computerization. But overall, new laws are needed to respond to technological change and the government's functions remain the same regardless of technology.

The Patriot Act and the National Surveillance State

As a response to the terrorism of September 11, the Patriot Act accelerated and strengthened the National Surveillance State. The Patriot Act unconstitutionally increased the ability of law enforcement agencies to search telephone and e-mail communications with minimal constitutional protections or legal precedent. Concerns have been raised about inadequate judicial supervision and the potential for

[30] *Id.* at 4.

unconstitutional interception of content information from electronic communications.[31] Much of that controversy stems from distinguishing between domestic law enforcement surveillance and foreign intelligence surveillance. As previously mentioned, this was caused by the Patriot Act's provisions on the relaxation of the "primary purpose" of the surveillance order. This change, coupled with the authorization of pen register and trap-and-trace expansion, roving wiretaps, "sneak-and-peek" warrants, and seizure of electronic voice-mail, have arguably expanded the National Surveillance State, which will be addressed in chapter three of this thesis.

As intelligence and law enforcement agencies continue to increase their communication by using modern technology pursuant to the Patriot Act, it is debatable whether the use of these technologies will constitute a threat to civil liberties or whether it is a better way to constitutionally prevent terrorism. On the one hand, conducting surveillance among agencies makes the job of law enforcement easier and allows for the discovery of crimes and terrorist plots that might not have otherwise been discovered. Sharing of data between intelligence services and federal, state and local law enforcement helps the government identify patterns of criminal activity, prevent crimes before they occur, and allow for more prosecutions. These new techniques and technologies allow governments to do the jobs entrusted to them more efficiently than ever before.

On the other hand, it can be argued that these developments carry risks for the government to make mistakes in assessing levels of threat and criminality and that their data mining models may characterize innocent activity as suspicious. Without sufficient

[31] Lisa M. Kaas, *Liberty v. Safety: Internet Privacy After September 11*, GEO. J. L. & PUB. POL'Y 1: 175 at 182 (2002).

oversight and checks on power, government actors may misuse the knowledge they gain such as instigating abusive prosecutions and creating discriminatory systems for access to public and private services.

Conclusion

The National Surveillance State is a theory that suggests that government will increase its collection of information from its citizens based on political conditions and the advances of technology. In this chapter, I examined the threats of this posed by this State and I discussed some possible ways to contain it. I also put forth an alternate view to the theory that this State exists. As Kerr suggests, it may not be a new form of government but rather a new way of doing what government has done for years.

I ended this chapter with the notion that legislation such as the Patriot Act, may contribute to the theory that a National Surveillance exists, a topic that will be discussed in the next chapter.

Chapter Two: Key Patriot Act Sections on Electronic Surveillance

In this chapter, I explore how the Patriot Act significantly changed electronic surveillance through an in-depth analysis of four key Patriot Act sections. Further, by reviewing the academic debate relevant to these changes I will assess the variety of viewpoints regarding this topic in order to determine the extent of the theory of a National Surveillance State.

Consequently, I argue that these Patriot Act sections, both collectively and separately, significantly increased the government's power to collect information on its citizens. I maintain that these changes may violate constitutional protections on electronic privacy. Both of these positions are consistent with the theory of a National Surveillance State. I also argue, however, Kerr's position that these Patriot Act sections would simply need minor adjustments to the law in order to address technological and constitutional challenges, instead of the enactment of "super-statutes" as proposed by Balking and Levinson.

Electronic Provision of the USA Patriot Act

Title II of the Patriot Act made several changes to U.S. law, specifically to the laws relating to foreign intelligence surveillance, which included FISA and the ECPA. Four key provisions specifically address electronic surveillance. These provisions have been the most significant and changes to federal electronic surveillance law. They

include sections 206-*Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978*, 209-*Seizure of voice-mail messages pursuant to warrants*, 216-*Modification of authorities relating to use of pen register and trap and trace devices*, and 218-*Foreign Intelligence Information.*

Section 206 the "Roving" Wiretap Provision

Section 206 of the Patriot Act amended FISA allowing for so-called "roving" wiretaps that allow for the FISA court to authorize intercepts on any phones or computers that a suspect may use. Before the Patriot Act was enacted, roving wiretaps were only available in the law enforcement context, which included Fourth Amendment protections such as notice and probable cause, and, to obtain one, the government had to show that the suspect was actually using the line to be tapped.[32] Section 206 changed this and now the government has the power to engage in roving surveillance without Fourth Amendment protections.

Another concern with this change is that roving wiretaps are suspect-specific rather than device-specific, meaning these wiretaps follow the suspect wherever he roams. This change means that the police no longer need to list the phone numbers to be tapped. Instead, the police can listen to all phones where the suspect works, shops, or visits.[33] The Federal Bureau of Investigation (FBI) responded to this change by saying

[32] 18 U.S.C. Section 2518(12) (2000).
[33] Erwin Chemerinsky, *Post 9/11 Civil Rights: Are Americans Sacrificing Freedom for Security?*, DENV. U. L. REV. 759: 759-774 (2004).

that roving wiretaps are necessary because the process of adding a new telephone number to an existing warrant, which requires court approval, takes too long.

Under this section, FISA warrants allow continuing surveillance of a terrorist suspect even if he switches communication devices and methods. Further, prior to the Patriot Act FISA warrants were only authorized within a single city or district; now they are authorized nationwide.[34] Therefore, the argument for roving wiretaps is that suspected terrorists might repeatedly change cell phones, thus eluding surveillance by wiretaps of specific phone numbers.[35]

The problem here is that there is no effective way to filter out the communications of innocent persons if, for example, the suspect enters another person's home and law enforcement officers believe he may use the phone lines there. Any inadvertent interception of an innocent party's communications becomes a violation of that party's Fourth Amendment rights.[36] According to Erwin Chemerinsky, Dean of the University of California at Irvine Law School, the problem with this provision is that the government can tap any telephone that the suspect is likely to use; therefore, any telephone that is near the suspect can be tapped. This provision essentially gives the government wide latitude of telephone surveillance, limited only by the traveling patter of the suspect. In response to terrorist evading wiretap orders, Chemerinsky argues that that there is a need to establish a faster procedure for judicial approval instead of creating an unrestricted roving wiretap.

---

[34] Currently, this provision was reauthorized and has a sunset of Dec. 31, 2009.
[35] *See* Chemerinsky, *supra* at note 33.
[36] *See* Kaas, *supra* at note 31, 187.

At the forefront of this debate are Internet privacy organizations such as the Electronic Privacy Information Center[37] (EPIC) and the Electronic Frontier Foundation (EFF). EPIC stated that "the private communications of law-abiding American citizens might be intercepted incidentally" and therefore the amendment violates the privacy protections against unreasonable searches and seizures.

On the other side of the debate are Georgetown University Law Center Professor David D. Cole and James X. Dempsey[38]. While a critic of many of the provisions of the Patriot Act, he found that, even though the roving wiretaps come at a cost to privacy, they are a sensible measure, [39]precisely because many suspects try to evade traditional wiretaps by using a cell phone or making use of several cell phones. This position is also supported by University of California Berkeley Law School Professor John Yoo. Yoo sees the roving wiretaps provision as a "common-sense" adjustment that modernizes existing laws like FISA to meet the new terrorist threat.[40] He explains that before the Patriot Act, the government had to seek an individual warrant for each communication device used by a terrorist suspect, and it had to get a new warrant each time a suspect traveled to a new judicial district.

Regardless of the arguments, roving wiretaps exemplify an increase of governmental surveillance powers. Whether roving wiretaps are a reasonable measure by the government is debatable, but that debate may miss the more crucial point that roving wiretaps have effectively eliminated judicial oversight in the name of efficiency and

---

[37] Electronic Privacy Information Center (EPIC), http://epic.org/privacy/wiretap/stats/wiretap_stats.html
[38] Vice President for Public Policy, Center for Democracy & Technology, www.cdt.org
[39] David Cole and James X. Dempsey, *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security*, NEWS PRESS (2006).
[40] John Yoo. *The Terrorist Surveillance Program and the Constitution*, Geo. Mason Law Rev., 14:565.

personal privacy. This is the underlying risk of the potential National Surveillance State; it effectively removes a check on governmental power. Another concern with the roving wiretap provision is that it excludes the requirement that an individual suspect be named in a FISA warrant application, giving rise to concerns about what have been dubbed "John Doe" warrants that specify neither a particular interception facility nor a particular, named suspect.[41]

This provision provides great concern because allowing roving surveillance to be conducted pursuant to FISA may result in the interception of numerous innocent conversations, many of which will involve U.S. persons. As a matter of general policy, this section leaves too much discretion to the Executive Branch.

Section 209 Seizure of Voice-Mail Messages

Prior to the Patriot Act, the Wiretap Act of 1968[42] (Title III) set forth procedures for court authorization of wiretap surveillance of electronic communications, including voice, e-mail, fax, and internet, in criminal investigations. These wiretap orders had stricter Constitutional requirements than warrants for physical searches. This high standard meant that a judge must conclude, based on evidence submitted by the government, that there is probable cause to believe that a crime *has been, is being, or is about to be committed.* Contrast this requirement to the lower standard of a regular

[41] Trevor W. Morrison, *The Story of United States .v United States District Court (Keith): The Surveillance Power*, Columbia Public Law Research Paper No. 08-189, 21 (2008).
[42] U.S.C. Title 18, Section 2510.

physical search warrant that merely requires that probable cause be established by an officer having either direct information about a crime or by obtaining hearsay of a crime.

The provisions of Title III were intended to expand the protections explicitly outlined in the Fourth Amendment by stating that American citizens have "a reasonable expectation of privacy" from the state. The privacy of "oral communications" is included under this "reasonable expectation" in Title III.

Under Section 209 of the Patriot Act, this type of electronic surveillance is now governed by the Electronic Communications Privacy Act (ECPA), a statute that gives you much less protection against government spying than Title III. Under this Act, the standard for a wiretap is downgraded to the establishment of probable cause as described previously.

Another result of this provision is that there is no rule to exclude this evidence in court under the ECPA. Prior to the Patriot Act, if the government listened to your voicemail illegally (without a valid warrant), it could not use the messages as evidence against you. But since the ECPA has no exclusionary rule, if the government gains access to your voicemail in violation of the statute, it can freely us it as evidence against you.[43] In addition, there is no longer a requirement to notify the suspect of this search. Therefore, the only way you will find out if the government uses your voicemail is if they use it against you in court.

Based on his "shift to computerization" view described in Chapter 1, Orin Kerr does not find this section of the Patriot Act to be a violation of privacy rules. Instead he believes that the ECPA "adopted a rather strange rule to regulate voicemail stored with

[43] Electronic Frontier Foundation (EFF), http://w2.eff.org/patriot/sunset/209.php

service providers," because "under ECPA, if the government knew that there was one copy of an unopened private message in a person's bedroom and another copy on their remotely stored voicemail, it was illegal for the FBI to simply obtain the voicemail, while the law actually compelled the police to invade the home and rifle through peoples' bedrooms so as not to disturb the more private voicemail." In his opinion, doing this made little sense, and the amendment under the Patriot Act was reasonable and sensible.[44]

Determining the privacy protection of voicemails poses a legal challenge that is open to debate. If the voicemail is treated like a "private letter" then it should be subject to a regular search warrant like all postal mail. On the other hand, if the voicemail is treated like electronic communication, then an argument can be made that a wiretap surveillance order is required. The latter has a higher threshold of proof by the government. Ultimately, it will be the courts that will determine whether the level of proof required by the government in order to conduct surveillance on voicemails. The determination of this requirement supports the argument that the contours of the National Surveillance State will be shaped by the courts, and in general they will accommodate to the laws created and enforced by the other two branches of government, according to Balkin and Levinson.

[44] Kerr, Orin, Patriot Debates Blog, American Bar Association, at: http://www.abanet.org/natsecurity/patriotdebates/209-212-and-220-2#rebuttal

Section 216 Pen Register/Trap & Trace Device Modification

Section 216 of the Patriot Act modified the definition of pen register and trap-and-trace devices[45]and changed it by expanding the use of these devices to include "dialing, routing, addressing, or signaling information" in order to encompass both telephones and the Internet. This modification was supplemented with a clarification that "such information shall not include the *contents* of any communication."[46] This clarification was necessary in order to distinguish the use of pen-registers and trap-and-trace from a wiretap order, which requires probable cause in order to eavesdrop on the communication.

Pen registers and trap and trace devices allow law enforcement officers to record the numbers of incoming and outgoing calls on a specific telephone. A log of the numbers of all phones called by one particular phone is called a pen register. Taking note of the numbers of all phones that call a particular phone is called trap-and-trace. This information can provide an analysis of telephone calls that can reveal the structures of organizations and the movements of people. Under ECPA, pen registers and trap-and-trace devices require court orders, but there is no requirement for probable cause for the search warrant. The main reason for not requiring probable cause is that unlike a wiretap the content of the conversation would not be invaded.

[45] Patriot Act Section 216.
[46] *See* 18 U.S.C.A. § 3127(3)-(4) (West Supp. 2002).

Every communication network features two types of information: the contents of communications, and the addressing and routing information that the networks use to deliver the contents of communications. The former is "content information," and the latter is "envelope information."[47] The essential distinction between content and envelope information remains constant across different technologies, from postal mail to email.[48] With postal mail, the content information is the letter itself, stored safely inside its envelope. In contrast, the envelope information is the information derived from the outside of the envelope, including the mailing and return addresses, the stamp and postmark, and the size and weight of the envelope when sealed.[49] According to Kerr, there is no reasonable expectation of privacy on the outside of postal mail envelops because the information is made public in order to provide delivery service. Therefore, the Fourth Amendment provides no privacy protection in this circumstance.

The phone conversation or the letter in the envelope are content information, similarly the message in the body of the email is content information that is protected by the Fourth Amendment. But the email carries addressing information in a "mail header." Mail headers are digital postmarks that accompany every email and carry information about the delivery of the mail, much like the outside of an envelope in postal mail.

When the government looks at an email transmission, the envelope portion of the email message consists of the Header and the Subject Line. Both of these fields reveal information that is directly related to the content of the message which is protected by the

[47] Kerr.
[48] Kerr.
[49] *See* 39 C.F.R. § 233.3(c)(1)(2002) (articulating an administrative procedure for obtaining a "mail cover," which is defined as "the process by which a nonconsensual record is made of any data appearing on the outside cover of any sealed or unsealed class of mail matter, or by which a record is made of the contents of any unsealed class of mail matter as allowed by law").

Fourth Amendment. Viewed as a whole, the email header (minus the subject line and thread-topic) provides information about the email that is roughly analogous to the routing information in telecommunications and postal mail.

Orin Kerr sees this provision not only as innocuous to privacy, but to the contrary, he argues that the provision provides additional protection for privacy. In postal mail, although envelope information is not protected by the Fourth Amendment, under Section 216, the law protects envelope information on email, making it a federal crime to collect this information without a court order.[50] This is why Kerr argues that this section offers additional protection of privacy. According to Kerr, if the pen register statute did not apply to the Internet, then email surveillance would be completely unregulated by federal privacy law. In other words, the Patriot Act now requires a court order, whereas before that requirement was not explicit in federal law.[5152]

Fred Cate, an Indiana University professor who specializes in privacy issues, is not convinced that an assurance that only "envelope information," through a court order, is being captured. "Unlike a phone call, you're suddenly revealing content." "It is impossible to obtain the address information without seeing the content of the data."[53] Because the Header and Subject line of an email message can disclose the content of the

---

[50] Kerr defines envelope surveillance as the To and From address on an email and the mail header information, minus the subject line.

[51] According to Kerr, this requirement is a step in the direction of protecting privacy. However, Kerr believes that this section should have required a higher threshold to obtain the court order that was required, such as the "specific and articulable facts" threshold required by section 2703 under the Crimes and Criminal Procedure code of the United States.

[52] See 18 U.S.C. § 2703(d) (requiring government to obtain a court order before ordering an Internet service provider to divulge records, and stating that the order must state "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation").

[53] Galvin, Kevin. *Why New Law Enforcement Powers Worry Civil Libertarians*, Seattle Times, December 6, 2001. http://archives.seattletimes.nwsource.com/cgi-bin/texis.cgi/web/vortex/display?slug=liberties06m&date=20011206

message, it is difficult to accept Kerr's position that this provision of the Patriot Act, by design, would provide for more privacy.

Neither pen registers nor trap and trace devices are governed by Title III because they do not intercept the content of telephone conversations.[54] Nor are they governed by the Fourth Amendment because a person making a telephone call has no reasonable expectation of privacy in the telephone number dialed since this information is of necessity revealed to the telephone company in order to make the call.[55]

Section 218 The "Significant Purpose" Change

The Patriot Act altered the "primary purpose" requirement, and FISA surveillance requests no longer have to establish that intelligence gathering is "the" purpose of the surveillance. All that is required now is that intelligence gathering be a "significant" purpose.[56]

Prior to the Patriot Act, electronic surveillance under the Foreign Intelligence Surveillance Act (FISA) required a showing that the "primary purpose" of the surveillance was to gather foreign intelligence and that the target (the person to be placed under surveillance) was an "agent of a foreign power."

The purpose of being explicit in this law was to ensure that citizens of the United States were protected against unreasonable searches and seizures as required by the

[54] United States v. N.Y. Tel. Co., 434 U.S. 159, 165-68 (1977).
[55] Smith v. Maryland, 442 U.S. 735, 740-46 (1979).
[56] Nathan C. Henderson, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications*, DUKE L.J., 52: 179 (2002).

Fourth Amendment. With these two FISA requirements, the purpose of the surveillance was not intended for the use by domestic law enforcement and it was not directed at citizens of the United States. With these restrictions, FISA warrant applications did not need to show probable cause of criminal activity, as required by the Fourth Amendment, because the purpose of the surveillance was foreign intelligence gathering.[57] In contrast, where the government's primary purpose was domestic criminal law enforcement, the government was required to satisfy the criminal probable cause standards set forth by the Fourth Amendment.[58]

To establish probable cause for law enforcement surveillance, the government had to show that the suspect of the search had either evidence of crime in his possession or else had committed a crime. The rationale behind these two sets of requirements is that the purpose of intelligence gathering surveillance is to help prevent terrorism by foreign agents who do not have constitutional protections, whereas domestic law enforcement surveillance is meant to combat crime and build a legal case against a defendant.

This change was the result of Section 218 of the Patriot Act which amended the FISA surveillance requirement of foreign intelligence from being "the primary purpose" to only "a significant purpose."[59] This change meant that a FISA surveillance order can now be issued even if it is motivated by a law enforcement purpose, which always requires Fourth Amendment protections such as probable cause, as long as foreign intelligence gathering is a "significant purpose." Because a FISA order request does not

[57] Cole, David. http://encarta.msn.com/sidebar_701713501/Is_the_Patriot_Act_Unconstitutional.html, accessed November 12, 2007.
[58] *Id.*
[59] Patriot Act section 218.

require a probable cause justification, this change promotes the potential for law enforcement officials to circumvent the constitutional protection of unreasonable searches and seizures.

From the standpoint of the Department of Justice, the Foreign Intelligence Surveillance Court (FISC) and some lower federal courts, the words "primary purpose" were interpreted to mean that any such information gathered by counterintelligence services could not be shared, except under rare circumstances, with law enforcement.[60] To satisfy the primary purpose requirement, the Department of Justice accordingly adopted procedures limiting contact between foreign intelligence agents in the FBI and federal prosecutors.[61] As mentioned previously, this separation of information was commonly referred to as a "wall"[62] between intelligence and law enforcement. The wall thus was mainly the result of (1) lower courts' interpretation of the original FISA's "purpose" provision; (2) the Justice Department's procedures for implementing the lower courts' interpretation; and (3) the restrictive interpretation of those procedures by Department officials and the FISA Trial Court.

The general purpose of the "wall" was to prevent law enforcement and counterintelligence officials from pooling their information. From a policy perspective, this "wall" gave the impression that constitutional protections, such as probable cause,

---

[60] John Yoo, *The Terrorist Surveillance Program and the Constitution*, 91 Geo. Mason Law Rev. 573-602 (2007).

[61] Richard H. Seamon and William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, HARV. J.L. & PUB. POL'Y 28: 319. 424 (2005).

[62] Critics of section 218 claim that it eliminated the "wall" between criminal law enforcement and foreign intelligence agencies. But according to Georgetown Law Professor David Cole, that is not true. Cole points out that FISA did not require such a wall before the Patriot Act was enacted. It did not previously bar prosecutors or law enforcement agents from turning over information to intelligence agents, nor did it stop foreign intelligence agents from sharing with criminal prosecutors evidence of crime that they had discovered in their investigations, whether under FISA or otherwise. Evidence obtained in FISA searches could be, and was, used in criminal trials long before the Patriot Act.

would be afforded to the suspect when the surveillance pertained to criminal investigations as opposed to intelligence gathering.

One of the subtle yet far-reaching changes made by the Patriot Act is the foreign intelligence purpose standard of FISA. Under section 218 of the Patriot Act, a FISA warrant may be issued so long as "a significant" purpose of the electronic surveillance is to gather foreign intelligence. By simply replacing the word "primary" with "significant," the probable cause requirement was relaxed.[63] Now, so long as officials from the Executive Branch certify that foreign intelligence gathering is *a significant* purpose of the FISA surveillance, rather than the *primary* purpose of the FISA surveillance, the threshold foreign intelligence purpose requirement is met, allowing the electronic surveillance to occur. This is a significant change because it disrupts FISA's balance between allowing governmental actors the ability to conduct surveillance as a means to safeguard national security, and protecting the Fourth Amendment rights of U.S. citizens to be free from unreasonable searches and seizures. By changing this one word from "primary" to "significant," the Patriot Act permits the government to intrude upon the privacy of Americans without demonstrating probable cause that a crime has been or is soon to be committed—and without sufficient judicial oversight of such invasive governmental action.[64]

The legislative history shows that Congress designed the original FISA's purpose provision to restrict not only the type of information that the government could use but

---

[63] David Hardin, *The Fuss over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA Under the Fourth Amendment*, GEO. WASH. L. REV. 71: 291. P. 294 (2003).
[64] Sharon H. Rackow, *How the USA Patriot Act will Permit Governmental Infringement Upon the Privacy of Americans in the Name of "Intelligence" Investigations*, U. PA. L. REV. 1651 (2001).

also the purpose for which the government could seek that information. By doing so, the enactment of the law presumes that some purposes of the electronic surveillance are improper.[65] Furthermore, the legislative history contains some statements that seemingly support the judicial primary purpose test even more directly. The FISA Court of Review quoted one such statement. The House report stated that surveillance authorized by the bill that was obtained by FISA "are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information."[66]

Analysis on the Increase of FISA Wiretap Applications and Orders

As predicted by many legal scholars, the number of FISA searches dramatically increased since the Patriot Act was passed, and for the first time now exceeds the number of wiretaps issued for domestic law enforcement (Title III). Further, in more than twenty years that have passed since FISA was enacted, only two applications have been rejected.[67] This is a landmark shift in the history of electronic surveillance because FISA wiretaps historically numbered far less than Title III law enforcement wiretaps prior to the Patriot Act. This shift may indicate that the National Surveillance State has significantly increased since the Patriot Act.

This increase in wiretaps from Title III to FISA is troublesome because FISA searches are conducted in secrecy. FISA's secrecy makes it difficult to hold government

[65] Richard H. Seamon and William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, HARV. J.L. & PUB. POL'Y 28: 319. 424. (2005).
[66] 310 F.3d 717 (2002).
[67] Steven Dycus et. Al., National Security Law 696 (3d ed. 2002).

accountable. The suspect of a search is never notified that he or she was searched, unless evidence from the search is subsequently used in a criminal prosecution. Even then, the defendant cannot see the contents of the application for the search, and therefore cannot meaningfully test its legality in court.[68] This places the defendant at a significant disadvantage in the judicial process because it shifts the burden of proof on the defendant while at the same time restricting access to that proof.

[68] *Id.*

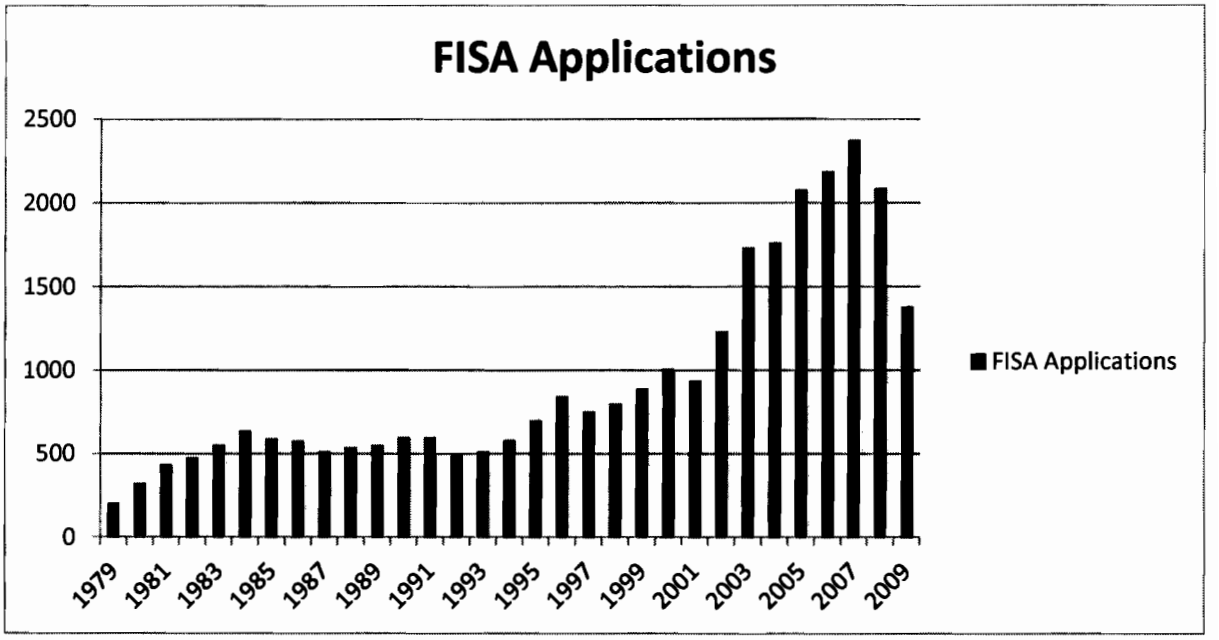

Figure 1.1. FISA Applications from 1979-2009.

Figure 1.1 illustrates the increase in trend of FISA applications since 2001. While it is difficult to pin-point a precise reason for the increase, it is important to note that the Patriot Act likely contributed to both the boost in applications and their subsequent approval of these applications. Such a sudden and rapid increase in FISA wiretaps makes it understandable why Balkin and Levinson believe that the Patriot Act served as a catalyst to a National Surveillance State.

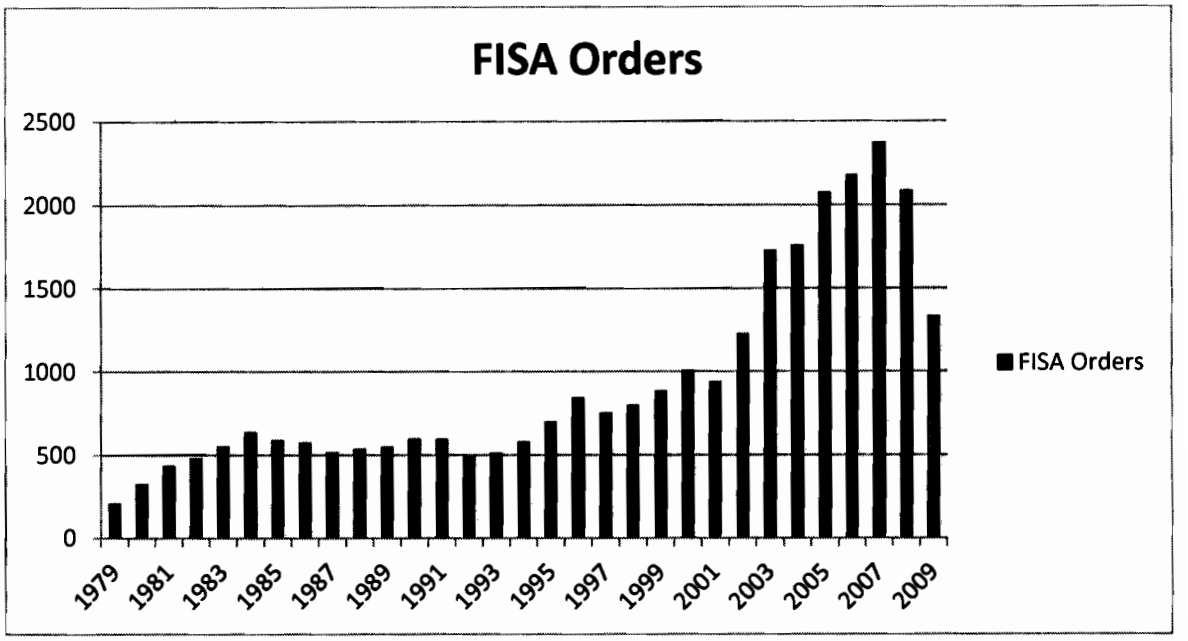

Figure 1.2. FISA Orders from 1979-2009.

In Figure 1.2, we see that the trend of approval for applications is near 100% (97% to be exact). Therefore, the approval of FISA orders more than doubled since the Patriot Act was enacted. Historically, FISA wiretap orders numbered far lower than law enforcement Title III wiretap orders, but in 2003 FISA wiretaps exceeded Title III wiretap orders and have continue to outpace.

FISA wiretaps have grown substantially in the past decade, especially after September 11. Since the early 1980s they have constituted the majority of federal wiretaps.[69] These graphs demonstrate that in 2003, for the first time, the number of surveillance orders issued under FISA exceeded the number of law enforcement wiretaps issued nationwide.[70]

Once the FISA system was up and running in 1981, there remained between 433 and 600 orders for each year through 1994, except for a one year total of 635 in 1984. In 1995, 697 orders were granted, growing in subsequent years to 839, 748, 796, 880, and 1012. FISA orders fell to 934 in 2001, and grew to record numbers of 1228 in 2002 and 1727 in 2003. Taken together, FISA wiretaps have grown substantially in the past decade, especially after September 11. Since the early 1980s they have constituted the majority of federal wiretaps. Because of the secret nature of FISA wiretaps, systematic reporting becomes more important. Without systemic reporting, it will be difficult to learn if the extraordinary powers of FISA are being used in new and potentially disturbing ways.

Conclusion

After gaining a better understanding of the intrusions that these Patriot Act sections will permit upon constitutionally protected civil liberties, particularly our Fourth Amendment, it is clear that Americans should not be so willing to give up these valued freedoms as a means to combat terrorism.

---

[69] Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, GEO. WASH. L. REV. 72: 1306 (2003).
[70] *Id.*

The concern raised by this amendment is that FISA will be used as a means to undertake surveillance without demonstrating the heightened standard of probable cause required under Title III for criminal wiretaps. FISA will be employed to approve investigations of predominantly criminal activities, including purely domestic criminal acts—in explicit violation of the Fourth Amendment.

In this chapter, I explored how four key Patriot Act sections significantly changed electronic surveillance. Based on the theory of a National Surveillance State explored in chapter two, each of these Patriot Act sections, collectively and separately, contributed to an increase in governmental collection of electronic information. This increase was demonstrated in the charts that reveal a spike in FISA wiretap applications and orders following the enactment of the Patriot Act.

Each of these sections, however, could have been modified to address the technological challenges in electronic surveillance and maintain constitutional electronic protections. As such, Kerr maintains that "super-statutes" are unnecessary when addressing electronic surveillance challenges due to updates in technology.

Chapter Three: Legal Background of Government Electronic Surveillance

In this chapter, I explore historical and contextual elements in relation to the development of electronic surveillance in order to place the theory of a National Surveillance State into an appropriate background for analysis. Analyzing the development of electronic surveillance is useful in determining if any patterns arise that influenced the theory of a National Surveillance State.

In order to fully develop this position, I provide a chronological examination of legal cases and acts of Congress that address issues pertaining to electronic surveillance. This analysis will demonstrate that the courts balanced the needs of national security with the principles of individual privacy afforded in the constitution. I argue that the Judicial and Legislative branches have played an active role in the conduct of governmental electronic surveillance and protection of individual privacy.

Case Law and Congressional Acts on Electronic Surveillance

In 1928, *Olmstead v. United States* became the first Supreme Court decision to address the issue of privacy and wiretaps. The government was secretly wiretapping the telephone conversations of bootleggers who were in violation of the National Prohibition Act. The Supreme Court ultimately decided that the Fourth Amendment, which protects against "unreasonable searches and seizures," was not violated because the wiretaps did not involve physical trespass on the suspect's property. The words of the Fourth

Amendment itself, the Court reasoned, "show that the search is to be of material things- the person, his house, his papers, or his effects." Because the government avoided any physical trespass on the defendant's property by wiretapping the phone lines through the wires outside his house, the Fourth Amendment was not implicated.

In his dissent of the opinion, Justice Brandeis cautioned against adopting too literal an interpretation of the Fourth Amendment. He argued that the protections guaranteed by the Fourth Amendment were "much broader in scope" than the majority had defined. Justice Brandeis maintained that the Framers of the Constitution "conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[71] This dissent was the first caution against conducting this early method of government electronic surveillance.

Taking note of the concerns expressed in Justice Brandeis' dissent, the Legislative branch responded in 1934 by passing the *Communications Act of 1934*. This act of Congress provided federal standards for the use of wiretaps. The law stated that "no person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[72] Basically, the law prohibited the interception and disclosure of any communication without the consent of at least one of the parties to the communication. This legislative response became the first attempt to protect the electronic privacy of citizens, as set forth in the Fourth Amendment.

---

[71] Olmstead v. United States, 277 U.S. 438, 466 (1928).
[72] 47 U.S.C. Section 605(a) (2000).

This initial response demonstrates that the Legislative branch took an active role in the protection of electronic privacy. Perhaps influenced by the dissent in *Olmstead*, Congress understood that unless it placed limits to wiretapping, a lure for widespread use of this form of electronic surveillance exists. In passing the *Communications Act of 1934*, Congress listened to the concerns of the Judicial branch and took measures to restore the balance between security and civil liberties. This response shows that both the Judicial and Legislative branches stand ready to intervene with constitutional principles to protect privacy, versus simply cooperating with the Executive branch, as the theory of the National Surveillance State maintains.

Despite this initial attempt to regulate federal wiretapping, State wiretapping practices and laws varied considerably during this period, and neither federal statutory nor constitutional rules applied to the states at the time. This created an inconsistency for wiretap requirements, and ambiguity in the standard for the conduct of wiretap surveillance. Consequently, state law enforcement officers were authorized wiretaps under the weaker standards of state laws, sometimes in violation of Fourth Amendment protections.[73]

By 1967, the Supreme Court revisited the issue of wiretapping and Fourth Amendment protection, this time testing a state law. In *Berger v. New York*, the Supreme Court reviewed the wiretapping laws of the state of New York. In *Berger*, the Court characterized as offensive any electronic surveillance that was "lengthy, continuous, or

[73] Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, GEO. WASH. L. REV. 72: 1306 (2003).

excessively broad."[74] The *Berger* opinion decided that in order for a state law on wiretapping to be constitutional, it must require that: a) "a neutral and detached authority" evaluate whether probable cause exists before wiretapping occurs; b) the application for the wiretap order must explain "what specific crime has been or is being committed, the place to be searched, and the persons or things to be seized"; c) the wiretap order "places a termination date" on the surveillance; d) there is "notice as [with] conventional warrants," or "some showing of special facts" to excuse notice; and e) there is "a return on the warrant."

The New York state statute, for wiretap surveillance, did not meet any of these requirements, therefore the Supreme Court found the state law unconstitutional. The most significant aspect of this decision is that the Supreme Court required judicial review ("a neutral and detached authority") to be part of the wiretap request process thereby creating a check on the Executive branch. All State wiretap laws were now subject to the tests laid out in the *Berger* case, initiating a more comprehensive standard for wiretap surveillance. Rather than simply cooperate with the request to conduct wiretaps, this case demonstrates that the Judicial and Legislative branch will ensure that constitutional requirements are met.

Shortly after the *Berger* decision, the Supreme Court decided in *Katz v. United States*[75]that the Fourth Amendment applied to "people, not places." This reversed the decision in *Olmstead*, which literally interpreted the Fourth Amendment definition of trespassing on a suspect's property. This is significant because the decision expanded

[74] 389 U.S. 347 (1967).
[75] *Id.*

privacy rights. So long as an individual can expect privacy in their telephonic conversation, the government is required to obtain a search warrant before conducting wiretap surveillance. The Fourth Amendment "extends as well to the recording of oral statements overheard without any technical trespass. The principal factor in whether an act of the government constituted a search or seizure under the Fourth Amendment lay not in the physical location of the action, but in whether the individual had a "reasonable expectation of privacy" within the circumstances.[76]

In response to the decisions made by the Judicial branch in *Berger* and *Katz*, Congress passed Title III of the *Omnibus Crime Control and Safe Streets Act of 1968* (Title III). In enacting Title III, Congress sought to protect privacy by establishing uniform conditions under which electronic surveillance, for the purpose of law enforcement, could occur. Most importantly, Title III established that the government could only intercept the content of wire communications pursuant to a court order based on a finding of probable cause. This made all governmental electronic surveillance related to crime control illegal, unless first authorized through a court order. Title III also mandated that the suspect under surveillance have the opportunity to challenge both the existence of probable cause and the conduct of the surveillance prior to the introduction of any damaging evidence in a criminal proceeding. Title III continues to apply to law enforcement wiretaps in the United States to this day.[77] However, since Title III applied solely to crime control, it did not address the use of wiretaps for intelligence gathering.

[76] Swire at 1313.
[77] *Id.* at 1311.

That issue was raised four years later in the case of *United States v. U.S. District Court*[78] (also known as the *Keith* case).

In *United States v. U.S. District Court*, better known as the *Keith*[79] case, the Supreme Court had to answer whether the President, acting in the interests of national security, may authorize the electronic surveillance of persons within the United States without first obtaining a judicial warrant?[80] The Court concluded that "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillance may be conducted solely within the discretion of the Executive Branch."[81] But the Court also limited its holding to cases involving "the domestic aspects of national security," and "expressed no opinion as to the surveillance of the activities of foreign powers or their agents."[82]

In the district court opinion, Judge Keith drew a distinction between surveillance targeting purely domestic entities and surveillance targeting foreign powers:

> An idea which seems to permeate much of the Government's argument is that a dissident domestic organization is akin to an unfriendly foreign power and must be dealt with in the same fashion. There is a great danger in an argument of this nature for it strikes at the very constitutional privileges and immunities that are inherent in United States citizenship. It is to be remembered that in our democracy all men are to receive equal justice regardless of their political beliefs or persuasions. The executive branch of our government cannot be given the power or the opportunity to investigate and prosecute criminal violations under two different standards simply

[78] 407 U.S. 297 (1972).
[79] "Keith" refers to Damon J. Keith, the federal district judge in the case.
[80] Trevor W. Morrison, *The Story of United States .v United States District Court (Keith): The Surveillance Power*, Columbia Public Law Research Paper No. 08-189, (2008).
[81] *Keith*, 407 U.S. at 316-17.
[82] *Id.* at 321-22.

> because certain accused persons espouse views which are inconsistent with our present form of government.[83]

The point is that the Fourth Amendment must apply fully to "dissident domestic organizations" precisely because such organizations are subject to the domestic criminal justice system. "Foreign powers," on the other hand, are not likely to face prosecutions in the U.S. courts.[84]

In *Keith*, the Supreme Court held that a warrant is necessary before conducting electronic surveillance even if domestic security issues, the justification for intelligence gathering, are involved. This is significant because the Supreme Court unanimously upheld the requirements of the Fourth Amendment for all types of electronic surveillance, thereby strengthening the protection of civil liberties.

Despite the Executive branch's plea to conduct domestic security electronic surveillance without a warrant, the Court rejected the argument and held that the facts of *Keith* did "not justify complete exemption of domestic security surveillance from prior judicial scrutiny." When conducting electronic surveillance for domestic security purposes, the Court held, the Fourth Amendment requires that the government first seek judicial approval from a neutral magistrate.[85]

Further, the Court expressly held that Congress had the power to set forth reasonable standards governing the warrant process for domestic national-security surveillance:

---

[83] *Id.* at 1079.
[84] *See* Morrison, *supra* note 80, at 1.
[85] Kathlyn Querubin, *Cutting the Fourth Amendment Loose from Its Moorings: The Unconstitutional Use of FISA Evidence in Ordinary Criminal Prosecutions*, HASTINGS CONST. L.Q. 385-386 (2009).

> We do not attempt to detail the precise standards for domestic security warrants any more than our decision in *Katz* sought to set the refined requirements for the specified criminal surveillances which not constitute Title III. We do hold, however, that prior judicial approval is required for the type of domestic security surveillance involved in this case and that such approval may be made in accordance with such reasonable standards as the Congress may prescribe.[86]

The Court however, explicitly stated that its holding was due in large part because the Fourth Amendment's protection of search and seizure applies only in *domestic* wiretapping. Based on this reasoning, the Legislative Branch saw this as a policy window of opportunity to pass a law that specifically distinguished foreign intelligence surveillance from domestic surveillance.

The Primary Purpose Test and the Creation of "The Wall"

Following the *Katz* decision, the courts had to grapple with the Executive branch's use of warrantless electronic surveillance on foreign intelligence. In general the courts held that the development of a test was required as a Fourth Amendment protection so long as the electronic surveillance was conducted for the sole or primary purpose of obtaining foreign intelligence information.[87] The test is associated with the decision in *United States v. Truong Dinh Hung* (*Truong*).[88] *Truong* is a significant case because it is the first decision to suppress evidence under this primary purpose test.[89]

---

[86] Katz v. U.S., 389 U.S. 347, 357 (1967).
[87] *See* Zweibon v. Mitchell, 516 F.2d 595 (1975).
[88] 629 F.2d 908 (4th Cir. 1980).
[89] Richard H. Seamon and William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, HARV. J.L. & PUB. POL'Y 28: 319, 362 (2005).

In *Truong*, the FBI tapped the phone and bugged the apartment of Mr. Truong for evidence that he was sending classified information to the government of Vietnam.[90] The FBI did not have a warrant or any other judicial authorization. The government used evidence gathered through the surveillance to convict Truong of espionage and other crimes. Truong challenged his convictions contending that the warrantless electronic surveillance violated his Fourth Amendment rights. The Fourth Circuit court reviewed the case and upheld the challenge in part, by stating that beginning on July 20, 1977, the investigation "became primarily a criminal investigation" and therefore any electronic surveillance from that point required a warrant.[91] The court however, upheld the admission of evidence prior to that date under a "foreign intelligence exception." This decision clarified that the purpose of gathering foreign intelligence information, through electronic surveillance, is incompatible with the purpose of obtaining evidence for prosecution.

Based on this decision, the court was uneasy about combining law enforcement and foreign intelligence gathering while conducting electronic surveillance. *Truong* therefore became the first case to differentiate law enforcement and foreign intelligence gathering by creating a "wall" while conducting electronic surveillance. As mentioned in Chapter USAPA, the Patriot Act changed the meaning for the purpose of electronic surveillance by changing it from "primary" to "significant." This change gives rise to the concern that a National Surveillance State may exist.

---

[90] *Truong*, 629 F.2d at 911-12.
[91] *Id.* at 916.

The Enactment of the Foreign Intelligence Surveillance Act (FISA)

Six years after the *Keith* case decision, Congress responded in 1978 by passing the Foreign Intelligence Surveillance Act (FISA)[92] FISA is sometimes viewed as a response to the Supreme Court's suggestion in *Keith* that Congress adopt special standards for surveillance in national security cases.[93] The Supreme Court expressly held that Congress had the power to set forth reasonable standards governing the warrant process for domestic national-security surveillance:

> Given the potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and protected rights of our citizens.[94]

FISA specifically establishes a framework for the use of electronic surveillance within the United States in order to acquire foreign intelligence information. It generally requires the government to obtain a judicial warrant before engaging in such surveillance and creates a special court (the FISA court, or FISC) for the issuance of such warrants. First, FISA is triggered only when surveillance is targeting a "United States person who is in the United States," or the surveillance "acquisition occurs in the United States."[95] FISA does not regulate electronic surveillance acquired abroad and targeted at non-U.S.

---

[92] Pub. L. No. 95-511, 92 Stat. 1783 (1978).
[93] *See generally* Robert Bloom & William J. Dunn, *The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment*, 15 Wm. & Mary Bill Rts. J. 147, 159 (2006).
[94] *Keith*, 407 U.S. at 322.
[95] 50 U.S.C. Section 1801(f)(1)-(2) (2000).

persons. Thus, it does not limit in any respect wholly foreign surveillance of al Qaeda, or indeed even of all persons in Afghanistan. Second, even when the target of surveillance in a U.S. person within the United States, or the information is physically acquired within the United States, FISA permits wiretaps approved by the FISA Court based on a showing of probable cause that the target is an "agent of a foreign power," which includes a member of a terrorist organization.

FISA used the terms "foreign power" and "agent of a foreign power" employed by the Supreme Court in *Keith*. These terms drew distinctions between U.S. persons and non-U.S. persons.[96] The former consists essentially of U.S. citizens and permanent residents. Non-U.S. persons could qualify as an "agent of a foreign power" simply by being an officer or employee of a foreign power, or a member of an international terrorist group.[97]

Through FISA, Congress created the Foreign Intelligence Surveillance Court (FISC) for the purpose of reviewing the Executive Branch's applications to conduct domestic surveillance for foreign intelligence gathering.[98] FISA authorizes the Chief Justice of the U.S. Supreme Court to appoint the eleven-member panel of the FISC from sitting district court judges.[99]

A significant problem with FISC is that it meets in secret and government petitions are heard in secret. In fact, the hearings are held *ex parte*, meaning that the government is the only party present at a FISA hearing. No opposing attorneys appear

---

[96] Swire 1310.
[97] *Id.* at 1321.
[98] Lance Davis, *The Foreign Intelligence Surveillance Court's May 17 Opinion: Maintaining a Reasonable Balance Between National Security and Privacy Interests,* MCGEORGE L. REV. 34: 713 (715).
[99] *Id.* at 716.

before the FISC's and opinions are almost never published.[100] As such, there is no public evidence to determine whether Fourth Amendment rights have been violated.

In fact, FISA establishes a reasonable procedure and expressly permits wiretapping of foreign agents, including members of international terrorist organizations and merely requires judicial confirmation that there is a factual basis for doing so. First, FISA is triggered only when surveillance is targeting a "United States Person who is in the United States," or the surveillance "acquisition occurs in the United States." FISA does not regulate electronic surveillance acquired abroad and targeted at non-U.S. persons. Thus, it does not limit in any respect foreign surveillance of al Qaeda, or of all persons in Afghanistan.[101]

Second, even when the target of surveillance is a U.S. person within the United States, or the information is physically acquired within the United States, FISA permits wiretaps approved by the FISC based on a showing of probable cause that the target is an "agent of a foreign power," which includes a member of a terrorist organization.

In summation, FISA represents Congress's determination to protect constitutional values by subjecting even foreign intelligence surveillance to the constraints of a judicial warrant procedure.[102] Just as *Keith* held that the Executive branch's authority to order domestic security surveillance was subject to the constraints of the Fourth Amendment, Congress in FISA exercised its authority to foreign intelligence electronic surveillance.

---

[100] *Id.*
[101] Michael Avery, *The Constitutionality of Warrantless Electronic Surveillance of Suspected Foreign Threats to the National Security of the United States*, U. MIAMI L. REV. 62: 541, 557 (2008).
[102] *See* Tracey Maclin, *The Bush Administration's Terrorist Surveillance Program and the Fourth Amendment's Warrant Requirement: Lessons from Justice Powell and the* Keith *Case*, 41 U.C. Davis L. Rev. 1259, 1296 (2008).

Additional Protection on Electronic Surveillance Privacy

Under FISA, law enforcement and intelligence officers had to ensure that their electronic surveillance did not pierce "the wall" that separated domestic law enforcement wiretaps from foreign intelligence gathering; however as technology developed during the 1980s, the federal government attempted to make the distinction easier by extending privacy protections to new electronic communications. In 1986 Congress passed The Electronic Communications Privacy Act of 1986 (ECPA). Whereas Title III applied to "wire" and "oral" communications, such as phone wiretaps and bugs, the ECPA extended many of the same Fourth Amendment protections to e-mail and other "electronic" communications.[103]

In addition, the ECPA extended the prohibition of the use of pen register and/or trap and trace devices. As described in chapter two, a pen register is an electronic device that records all phone numbers dialed from a particular phone, while a trap and trace device records all numbers that are received by a particular phone. The use of either device by the government requires a search warrant.

In *Kyllo,*[104] the government suspected that marijuana was being grown in Danny Lee Kyllo's home. As a result, government agents used a thermal-imaging device to scan his home in order to detect any heat emanating from high-intensity lamps typically used for indoor marijuana growth. The scan showed that Kyllo's garage roof and a side wall were relatively hot compared to the rest of his home. Based in large part on the thermal

[103] *Id.* at 1312.
[104] Kyllo v. United States, 533 U.S. 27, 47 (2001).

imaging, a federal judge issued a warrant to search Kyllo's home where the agents subsequently found marijuana growing.

Kyllo was indicted on a federal drug charge and he unsuccessfully attempted to suppress the evidence on the basis that his privacy rights were violated. During the appeal the circuit court affirmed the decision stating that Kyllo did not have a reasonable expectation of privacy because he was not attempting to conceal the heat. Further, the circuit court stated that even if Kyllo tried to conceal the heat, the emanations of the hot spots were too amorphous to violate his privacy expectations. The Supreme Court granted a review of the appeal and with a five-to-four vote, reversed the circuit court's decision.

The Supreme Court decision held that technology not in "general public use," in this case a thermal imaging device used by law enforcement could not be used to establish the requisite probable cause to obtain a search warrant.[105] The use of the thermal imaging device was therefore considered a warrantless "search" in violation of the Fourth Amendment. A key premise behind this holding is that the information about the interior of the home could not otherwise have been obtained without an actual "physical intrusion into a constitutionally protected area" in this case the home.

Kyllo followed the Supreme Court's logic in *Katz,* which protected private conversations in a telephone booth, because although the surveillance technology only picked up emanations from the exterior of the house in *Kyllo*, there was still a protected

[105] Lisa M. Kaas, *Liberty v. Safety: Internet Privacy After September 11*, GEO. J. L. & PUB. POL'Y 1: 175 (2002).

Fourth Amendment right, reiterating that this right "protects people, not places."[106] In *Kyllo*, Justice Scalia gives considerable weight to the notion of future technological advancements that may be able to unobtrusively "see" into the privacy of the home.[107]

Until the *Kyllo* case, Title III and the ECPA rules remained largely unchanged. The essential structure of Title III and the ECPA remains in effect today, including the requirement of judicial supervision of wiretaps and the need for law enforcement to give suspects notice that a wiretap has been conducted on them.

Conclusion

The development of electronic surveillance emerged incrementally over time and unlike other issues related to privacy, technology kept Congress and the especially the courts active in determining the constitutional contours of individual electronic privacy. An extensive understanding of these cases and Congressional Acts is important in order to carefully evaluate whether the courts would simply cooperate with Acts of Congress and the Executive Branch, as suggested by the theory of a National Surveillance State, or rather, would the courts actively redefine the parameters of electronic privacy informed by the Constitution.

In this chapter I explored the development of electronic surveillance and discovered emerging patterns that suggest that the courts, in fact, do play an active role in defining constitutional limits on electronic surveillance by law enforcement and foreign

[106] 277 U.S. 438 (1928).
[107] Kyllo v. United States, 533 U.S. 27, 47 (2001).

intelligence. While the government is becoming more efficient in collecting information on potential suspects, the courts are ensuring that traditional constitutional protections, such as privacy, are not eliminated.

Technology, however, increasingly began to surge ahead of what statute could protect, especially where electronic communications were concerned. As a result, communications were subject to "widely disparate legal treatment" depending on the form of the communication. Recognizing the need for reform, Congress passed the Electronic Communications Privacy Act of 1986 (ECPA) in an attempt "to bring [the] new technologies...into the statutory framework of the laws governing wiretaps."

Keith and FISA share an overarching and significant similarity: an unwillingness to grant the Executive branch exclusive, unchecked power to engage in electronic surveillance in the name of national security.

Proposals and Conclusion

Proposals

In the context of the National Surveillance State, certain electronic surveillance legislation reduces individual privacy interests. Based on the concerns raised by this study, I set forth the following three proposals that may begin to mitigate areas of constitutional concerns.

First, electronic communication and surveillance legislation should be amended to include the exclusionary rule. The exclusionary rule, which is rooted in the Fourth Amendment, is a long-standing legal principle that makes evidence inadmissible if collected in violation of constitutional principles. As discussed in chapter two, the Patriot Act allowed for certain electronic surveillance laws to circumvent the exclusionary rule. However, without the exclusionary rule, there is little incentive for the government to follow the rules of evidence when conducting electronic surveillance.

Second, electronic communication and surveillance legislation should be amended to increase the use of minimization procedures. Minimization procedures limit the amount of surveillance information that can be retained and disseminated to include only relevant material. Effective minimization procedures would reduce the retention and dissemination of information collected that is outside of the scope of surveillance. These procedures would assist in protecting the privacy of innocent individuals who are not the target of the surveillance.

Lastly, I propose amending FISA to require the FISC to become an adversarial court that would allow for competing arguments to be heard in front of an independent judicial body. The current system is purely *ex parte*, meaning that only the government's argument is heard in front of the FISC. The court hearings can still be considered classified information for national security purposes, but there are now competing viewpoints that a judge can consider before rendering a final decision. Under the current system, the FISC is approving over 97% of FISA wiretap requests.

Conclusion

The current study began as an effort to understand the theory of a National Surveillance State, in particular, to determine if and how the development of electronic surveillance contributed to this theory of governance.

In chapter one, I reviewed and discussed the formation of a National Surveillance State according to Professors Balkin and Levinson. I argue that, while some electronic surveillance legislation is necessary to keep up with advances in technology for national security, Judicial and Legislative branches must respond to potential overreaching by the Executive branch in this field.

In chapter two, I analyzed four specific sections of the Patriot Act in order to determine their significance in the National Surveillance State. These sections either eliminated or relaxed previous constitutional standards that protected privacy rights. The Patriot Act also blurred the long standing distinction between criminal justice and foreign intelligence gathering; thereby reducing constitutional protections.

Lastly, in chapter three, I outlined the legal history and use of electronic surveillance by the government. The historical examination revealed that, while government rapidly developed and implemented new electronic surveillance technology, the Judicial and Legislative branches consistently addressed constitutional concerns, and at times, limited the Executive branch from using certain methods and technologies related to electronic surveillance. This is inconsistent with Balkin and Levinson's theory that the Judicial and Legislative branches would simply allow the Executive branch to overreach its authority. I argue that the courts and Congress consistently limited the Executive branch from unreasonable collection of information. Nevertheless, it is evident from legislation, such as the Patriot Act, that the collection of information by the government has significantly increased in scope and substance, supporting the argument that a National Surveillance State exists.

In conclusion, I believe that a delicate balance exists between privacy interests and national security concerns. Balkin and Levinson's theory of a National Surveillance State raises important concerns regarding electronic surveillance and its impact on privacy rights. However, I also agree with Kerr that, in order for the government to be effective in responding to national security concerns, it must have the ability to employ the appropriate technology to identify and eliminate threats. The need for electronic surveillance is evident, yet it should be conducted within the context of constitutional protections of individual rights and political checks and balances.

References

Books and Articles

Avery, Michael. 2008. "The Constitutionality of Warrantless Electronic Surveillance of Suspected Foreign Threats to the National Security of the United States." *University of Miami Law Review* 62: 541.

Balkin, Jack M. 2008. "The Constitution in the National Surveillance State." *Minnesota Law Review* 93: 1.

Balkin, Jack M. and Sanford V. Levinson. 2006. "The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State." *Fordham Law Review* 75: 489.

Chemerinsky, Erwin. 2004. "Post 9/11 Civil Rights: Are Americans Sacrificing Freedom for Security?" *Denver University Law Review* 759: 759-774.

Cole, David, and James X. Dempsey. 2006 Terrorism *and the Constitution: Sacrificing Civil Liberties in the Name of National Security.* New Press.

Davis, Lance. 2002. "The Foreign Intelligence Surveillance Court's May 17 Opinion: Maintaining a Reasonable Balance Between National Security and Privacy Interests." *McGeorge Law Review* 34: 713.

Hardin, David. 2003. "The Fuss over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA Under the Fourth Amendment." *George Washington Law Review* 71: 291.

Henderson, Nathan C. 2002. "The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications." *Duke L.J.* 52: 179.

Kaas, Lisa M. 2002. "Liberty v. Safety: Internet Privacy After September 11." *Georgetown Journal of Law and Public Policy* 1: 175.

f

Kerr, Orin S. 2003. "Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't." *Northwestern University Law Review* 97: 607.

Kerr, Orin S. 2003. "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution." *Michigan Law Review* 102: 801.

Kerr, Orin S. 2003. "Foreword: The Future of Internet Surveillance Law." *George Washington Law Review* 72: 1139.

Kerr, Orin S. 2009. "The National Surveillance State: A Response to Balkin." *Minnesota Law Review*

McCarthy, Michael T. 2002. "Recent Developments-USA PATRIOT Act." *Harvard Journal on Legislation* 39: 435.

Querubin, Kathlyn. 2010. "Cutting the Fourth Amendment Loose from Its Moorings: The Unconstitutional Use of FISA Evidence in Ordinary Criminal Prosecutions." *Hastings Constitutional Law Quarterly* 37: 371.

Seamon, Richard H. and William Dylan Gardner. 2005. "The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement." *Harvard Journal of Law and Public Policy* 28: 319.

Slobogin Christopher and Joseph E. Schumacher. 1992. "Reasonable Expectation of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society." *Duke Law Journal* 42: 727.

Swire, Peter P. 2003. "The System of Foreign Intelligence Surveillance Law." *George Washington Law Review* 72: 1306.

Yoo, John. 2006. "Courts at War." *Cornell Law Review* 91: 573-602.

Yoo, John. 2007. "The Terrorist Surveillance Program and the Constitution." *George Mason Law Review* 14: 565.

Cases

ACLU v. NSA, US District Court, Eastern District of Michigan, Southern Division, Case No. 06-CV-10204.

Berger v. United States, 388 U.S. 41 (1967).

Ex parte Milligan, 71 U.S. (4 Wall.) 2 (1866).

Hamdi v. Rumsfeld, 542 U.S. 507 (2004).

In re Sealed Case, 310 F.3d at 72-30.

Katz v. United States, 389 U.S. 347, 357 (1967).

Kyllo v. United States, 533 U.S. 27, 47 (2001).

Miranda v. Arizona, 384 U.S. 436 (1966).

Nardone v. United States, 302 U.S. 379 (1937).

Olmstead v. United States, 27 U.S. 438, 466 (1928).

Rasul v. Bush, 542 U.S. 466 (2004).

Rumsfeld v. Padilla, 542 U.S. 426-451 (2004).

Schenck v. United States, 249 U.S. 47 (1919).

Schmerber v. California, 384 U.S. 757 (1966).

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

United States v. United States District Court, 407 U.S. 297-318 (1972).

Zweibon v. Mitchell, 516 F.2d 595 (1975).

Congressional Legislation

Alien and Sedition Act of 1798, 5 Congress Ch. 74, 1 Statute 596 (expired 1801).

Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified).

The Communications Act of 1934.

The Electronic Communications Privacy Act of 1986.

Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §2510-2522.

Public Law 107-56 (Oct. 26, 2001) "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.

United States Constitution.

United States Senate, Select Committee to Study Governmental Operations with respect to Intelligence Activities, Hearings, November 18, 19, December 2, 3, 9, 10, 11, 1975, Ninety-Fourth Congress, First Session, 1975.

Government Books

108th Cong., "Privacy and Civil Liberties in the Hands of the Government Post-September 11, 2001: Recommendation of the 9/11 Commission.

109th Cong., Defense Technology and Privacy Advisory Committee." 108th Cong. 113 (2004). "Reauthorization of the USA Patriot Act (continued)." 109th Cong. 109-29 (2005).

Videos

Yoo, John and John Sims. 2007. Debate: FISA and Electronic Surveillance- Does National Security Burden Freedom? *University of the Pacific, McGeorge School of Law*. KF 4850.F575 (2007).

Further Readings

Books and Articles

Abdolian, Lisa Finnegan & Harold Takooshian. 2002. "The USA PATRIOT Act: Civil Liberties, the Media, and Public Opinion." *Fordham Urban Law Journal* 30: 1429.

Amar, Akhil Reed and Vikram David Amar. 2001. "The New Regulation Allowing Federal Agents to Monitor Attorney-Client Conversations: Why It Threatens Fourth Amendment Values." *Connecticut Law Review* 34: 1163.

Armist, Gail. 1989. "*Freitas* after *Villegas*: Are "Sneak-and-Peek" Search Warrants Clandestine Fishing Expeditions? *San Diego Law Review* 26: 933.

Baker, Thomas E. and John F. Stack Jr. 2006. *At War with Civil Rights and Civil Liberties.* New York: Rowman & Littlefield Publishers, Inc.

Banks, William C. 2002. "And the Wall Came Tumbling Down: Secret Surveillance After the Terror." *University of Miami Law Review* 57: 1147.

Baumgartner, Frank R. & Bryan D. Jones. 1993. *Agendas and Instability in American Politics.* Chicago: The University of Chicago Press.

Bigel, Alan I. 1986. *The Supreme Court on Emergency Powers, Foreign Affairs, and Protection of Civil Liberties 1935-1975.* New York: University Press of America.

Bloom, Elise M. and Madeline Schacter & Elliot H. Steelman. 2002. "Competing Interests in the Post 9-11 Workplace: The New Line Between Privacy and Safety." *William Mitchell Law Review* 29: 897.

Blum, Stephanie C. 2009. "What Really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform." *Boston University Public Interest Law Journal* 18: 269.

Bradley, Alison A. 2002. "Extremism in the Defence of Liberty?: The Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT ACT." *Tulane Law Review* 77: 465.

Bradley, Curtis A. and Jack L. Goldsmith. 2005. "Congressional Authorization and the War on Terrorism." *Harvard Law Review* 118: 2047.

Breglio, Nola K. 2003. "Leaving FISA Behind: The Need To Return to Warrantless Foreign Intelligence Surveillance." *Yale Law Journal* 113: 179.

Brown, William F. and Americo R. Cinquegrana. 1985. "Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment." *Catholic University Law Review* 35: 97.

Burkoff, John M. 2004. "A Flame of Fire": The Fourth Amendment in Perilous Times." *Mississippi Law Journal* 74: 631.

Cassidy, Charlie & Cassandra Porsch. 2002. "Government Monitoring of Attorney-Client Communications in Terrorism-Related Cases: Ethical Implications for Defense Attorneys." *Georgetown Journal of Legal Ethics* 17: 681.

Cinquegrana, Americo R. 1988. "The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978." *University of Pennsylvania Law Review* 137: 793.

Cohn, Marjorie. 2002. "The Evisceration of the Attorney-Client Privilege in the Wake of September 11, 2001." *Fordham Law Review* 71: 1233.

Corr, Kevin. 1995. "Sneaky But Lawful: The Use of Sneak and Peek Search Warrants." *University of Kansas Law Review* 43: 435.

Davis, Darren W. and Brian D. Silver. 2004. "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America." *American Journal of Political Science* 28-46.

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

Dean, Susan W. 2003. "Government Surveillance of Internet Communications: Pen Register and Trap and Trace Law Under the Patriot Act." *Tulane Journal of Technology & Intellectual Property* 5: 97.

Dhillon, Joginder S. and Robert I. Smith. 2001. "Defensive Information Operations and Domestic Law: Limitations on Government Investigative Techniques." *Air Force Law Review* 50: 135.

Dowley, Michael F. 2002. "Government Surveillance Powers Under the USA PATRIOT Act: Is It Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War." *Suffolk University Law Review* 36: 165.

Evans, Jennifer C. 2001. "Hijacking Civil Liberties: The USA PATRIOT Act of 2001." *Loyola University of Chicago Law Journal.* 33: 933.

Ewing, Alphonse B. 2002. "The USA Patriot Act." New York: Novinka Books.

Gauthier, Geraldine. 2002. "Dangerous Liaisons: Attorney-Client Privilege, The Crime-Fraud Exception, ABA Model Rule 1.6 and Post-September 11 Counter-Terrorist Measures." *Brooklyn Law Review* 68: 351.

Gouvin, Eric J. 2003. "Bringing Out the Big Guns: The USA PATRIOT Act, Money Laundering, and the War on Terrorism." *Baylor Law Review* 55: 955.

Grossman, Joel B. 1997. "The Japanese American Cases and the Vagaries of Constitutional Adjudication." *Hawai'i Law Review* 19: 649.

Henderson, Nathan C. 2002. "The PATRIOT Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications." *Duke Law Journal* 52: 179.

Herman, Susan N. 2005. "The USA PATRIOT Act and the Subjmajoritarian Fourth Amendment." *Harvard Civil-Liberties Civil-Rights Law Review* 67: 132.

Ignatieff, Michael. 2004. *Political Ethics in an Age of Terror: The Lesser Evil.* Princeton: Princeton University Press.

Kennedy, Charles H. and Peter P. Swire. 2002. "State Wiretaps and Electronic Surveillance After September 11." *Hastings Law Journal* 54: 971.

Konovalov, Paul V. 1996. "On a Quest for Reason: A New Look at Surreptitious Search Warrants." *Hastings Law Journal* 48: 435.

Ku, Ray and Raymond Shih. 2001. "The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance." *Minnesota Law Review* 86: 1325.

Lawrence, Paul S. 2002 "Kyllo: As Libertarian Defense Against Orweillian Enforcement." *Georgetown Journal of Law and Public Policy* 1: 155.

Lee, Laurie T. 2003. "The USA PATRIOT Act and Telecommunications: Privacy Under Attack." *Rutgers Computer & Technology Law Journal* 29: 371.

Leone, Richard C., and Greg Anrig, Jr. 2003. *The War on Our Freedoms: Civil Liberties in an Age of Terrorism.* New York: Public Affairs.

Madrinan, Peter. 2002. "Devil in the Details: Constitutional Problems Inherent in the Internet Surveillance Provisions of the USA PATRIOT Act of 2001." *University of Pittsburg Law Review* 62: 783.

Maggs, Gregory E. 2006. "The Rehnquist Court's Noninterference with the Guardians of National Security." *George Washington Law Review* 74: 1122.

McCarthy, Thomas R. 2001. "Don't Fear Carnivore: It Won't Devour Individual Privacy." *Missouri Law Review* 66: 827.

McGee, Jim. 1996. "How Drugs Sucked in the Army," *Manchester Guardian Weekly*, December 29, 1996, p. 12.

Mell, Patricia. 2002. "Big Brother at the Door: Balancing National Security with Privacy Under the USA PATRIOT Act." *Denver Law Review* 80: 375.

Merl, Seth R. 2001. "Internet Communication Standards for the 21st Century: International Terrorism Must Force the U.S. to Adopt "Carnivore" and New Electronic Standards." *Brooklyn Journal of International Law* 27: 245.

Muller, Eric L. 2001. "12/7 and 9/11: War, Liberties, and the Lessons of History." *West Virginia Law Review* 104: 571.

Nance, Aaron. 2001. "Taking the Fear Out of Electronic Surveillance in the New Age of Terror." *University of Missouri-Kansas City Law Review* 70: 751.

O'Connor, Michael P. and Celia Rumann. 2002. "Going, Going, Gone: Sealing the Fate of the Fourth Amendment." *Fordham International Law Journal* 26: 1234.

Osher, Steven A. 2003. "Privacy, Computers and the PATRIOT Act: The Fourth Amendment Isn't Dead, But No One Will Insure It." *Florida Law Review* 54: 521.

Palay, Marc. 1976. "The Fourth Amendment and Judicial Review of Foreign Intelligence Wiretapping: Zweibon v. Mitchell." *George Washington Law Review* 45: 55.

Pikowsky, Robert A. 2002. "An Overview of the Law of Electronic Surveillance Post September 11, 2001." *Law Library Journal* 94: 601.

Pisous, Richard M. 2006. *The War on Terrorism and the Rule of Law.* Los Angeles: Roxbury Publishing Company.

Posner, Eric A. and Adrian Vermeule. 2007. *Terror in the Balance: Security, Liberty, and the Courts.* Oxford University Press, New York, New York.

Posner, Richard A. 2002. "Pragmatism versus Purposivism in First Amendment Analysis." *Stanford Law Review* 737-741.

Posner, Richard A. 2006. *Not a Suicide Pact: The Constitution in a Time of National Emergency.* Oxford University Press, New York, New York.

Podger, Ellen S. & John Wesley Hall. 2002. "Government Surveillance of Attorney-Client Communications: Invoked in the Name of Fighting Terrorism." *Georgetown Journal of Legal Ethics* 17: 145.

Rackow, Sharon H. 2002. "How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of "Intelligence" Investigations." *University of Pennsylvania Law Review* 1651-1696.

Rehnquist, William H. 1998. *All the Law but One: Civil Liberties in Wartime.* New York: Vintage Books.

Reza, Sadiq. 2001. "Privacy and the Post-September 11 Immigration Detainees: The Wrong to a Right (and Other Wrongs)." *Connecticut Law Review* 34: 1169.

Saito, Natsu T. 2002. "Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and the Unlawful Repression of Political Dissent." *Oregon Law Review* 81: 1051.

Sims, John Cary. 2005. "What NSA Is Doing...and Why It's Illegal." *Hastings Constitutional Law Quarterly* 33: 105.

Sims, John Cary. 2007. "How the Bush Administration's Warrantless Surveillance Program Took the Constitution on an Illegal, Unnecessary, and Unrepentant Joyride." *UCLA Journal of International Law and Foreign Affairs* 12: 163.

Smith, Jeremy. 2003. "The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security." *North Carolina Law Review* 82: 412.

Solove, Daniel J. 2003. "Reconstructing Electronic Surveillance Law." *George Washington Law Review* 72: 1264.

Solove, Daniel J. 2008. "Data Mining and the Security-Liberty Debate." *University of Chicago Law Review* 74: 343.

Stone, Geoffrey R. 2004. *Perilous Times: Free Speech in Wartime From the Sedition Act of 1798 to the War on Terrorism.* New York: W.W. Norton & Company.

Stone, Geoffrey R. 1976. "The Scope of the Fourth Amendment: Privacy and the Police Use of Spies, Secret Agents, and Informers." *American Bar Foundation Research Journal* 1193-1240.

Swire, Peter P. 2003. "Katz is Dead. Long Live Katz." *Michigan Law Review* 102: 904.

Voors, Matthey Parker. 2002. "Encryption Regulation in the Wake of September 11, 2001: Must We Protect National Security at the Expense of the Economy?" *Federal Communications Law Journal* 55: 331.

Walker Jr., John Kent. 1986. "Covert Searches." *Stanford Law Review* 39: 545.

Warren, Samuel D. and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 193.

Weibgen, Lara. 2005. *The Reference Shelf 2005: The U.S. National Debate Topic 2005-06: U.S. Civil Liberties.* New York: H.W. Wilson.

Whitehead, John W. and Steven H. Aden. 2001. "Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives." *American University Law Review* 51: 1081.

Young, Mark G. 2001. "What Big Eyes and Ears You Have!: A New Regime for Covert Governmental Surveillance." *Fordham Law Review* 70: 1017.

Appendix A: Select Sections of the Patriot Act

115 STAT. 272 PUBLIC LAW 107–56—OCT. 26, 2001

UNITING AND STRENGTHENING AMERICA BYPROVIDING APPROPRIATE TOOLS REQUIREDTO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001

TITLE II--ENHANCED SURVEILLANCE PROCEDURES

SECTION. 206. ROVING SURVEILLANCE AUTHORITY UNDER THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978.

Section 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)(2)(B)) is amended by inserting, "or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons," after "specified person".

SECTION. 209. SEIZURE OF VOICE-MAIL MESSAGES PURSUANT TO WARRANTS.

Title 18, United States Code, is amended--

(1) in section 2510—

(A) in paragraph (1), by striking beginning with "and such" and all that follows through "communication"; and

(B) in paragraph (14), by inserting "wire or" after "transmission of"; and

(2) in subsections (a) and (b) of section 2703—

(A) by striking "Contents of electronic" and inserting "Contents of wire or electronic" each place it appears;

(B) by striking "contents of an electronic" and inserting "contents of a wire or electronic" each place it appears; and

(C) by striking "any electronic" and inserting "any wire or electronic" each place it appears.

SECTION. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.

(a) General Limitations.--Section 3121(c) of title 18, United States Code, is amended—

(1) by inserting "or trap and trace device" after "pen register";

(2) by inserting ", routing, addressing," after "dialing"; and

(3) by striking "call processing" and inserting "the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications".

(b) Issuance of Orders.—

(1) In general.--Section 3123(a) of title 18, United States Code, is amended to read as follows:

"(a) In General.—

"(1) Attorney for the government.--Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

"(2) State investigative or law enforcement officer.--Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

"(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify—

"(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

"(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

"(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

"(iv) any information which has been collected by the device. To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

"(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof)."

(2) Contents of order.--Section 3123(b)(1) of title 18, United States Code, is amended—

(A) in subparagraph (A)—

(i) by inserting "or other facility" after "telephone line"; and

(ii) by inserting before the semicolon at the end "or applied"; and

(B) by striking subparagraph (C) and inserting the following:

"(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and".

(3) Nondisclosure requirements.--Section 3123(d)(2) of title 18, United States Code, is amended—

(A) by inserting "or other facility" after "the line"; and

(B) by striking ", or who has been ordered by the court" and inserting "or applied, or who is obligated by the order".

(c) Definitions.—

(1) Court of competent jurisdiction.--Section 3127(2) of title 18, United States Code, is amended by striking subparagraph (A) and inserting the following:

"(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or".

(2) Pen register.--Section 3127(3) of title 18, United States Code, is amended—

(A) by striking "electronic or other impulses" and all that follows through "is attached" and inserting "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"; and

(B) by inserting "or process" after "device" each place it appears.

(3) Trap and trace device.--Section 3127(4) of title 18, United States Code, is amended—

(A) by striking "of an instrument" and all that follows through the semicolon and inserting "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;"; and

(B) by inserting "or process" after "a device".

(4) Conforming amendment.--Section 3127(1) of title 18, United States Code, is amended—

(A) by striking "and"; and

(B) by inserting ", and 'contents' " after "electronic communication service".

(5) Technical amendment.--Section 3124(d) of title 18, United States Code, is amended by striking "the terms of".

(6) Conforming amendment.--Section 3124(b) of title 18, United States Code, is amended by inserting "or other facility" after "the appropriate line".

SECTION. 218. FOREIGN INTELLIGENCE INFORMATION.

Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking "the purpose" and inserting "a significant purpose".

Appendix B: Select Sections of Title 18 as amended by the Patriot Act

U.S. CODE TITLE 18—CRIMES AND CRIMINAL PROCEDURE

PART I—CRIMES

CHAPTER 119—WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

SECTION 2510

As used in this chapter—

(1) "wire communication" means any aural transfer 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 (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

SECTION 2703

(a) Contents of Wire or Electronic Communications in Electronic Storage.— A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of Wire or Electronic Communications in a Remote Computing Service.—

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

PART II—CRIMINAL PROCEDURE

CHAPTER 206—PEN REGISTERS AND TRAP AND TRACE DEVICES

SECTION 3121. GENERAL PROHIBITION ON PEN REGISTER AND TRAP AND TRACE DEVICE USE; EXCEPTION

(c) Limitation.— A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

SECTION 3122. APPLICATION FOR AN ORDER FOR A PEN REGISTER OR A TRAP AND TRACE DEVICE

(a) Application.—

(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

SECTION 3123. ISSUANCE OF AN ORDER FOR A PEN REGISTER OR A TRAP AND TRACE DEVICE

(a) In General.—

(1) Attorney for the government.— Upon an application made under section 3122 (a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is

serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

(2) State investigative or law enforcement officer.— Upon an application made under section 3122 (a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(3)

(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify—

(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

(iv) any information which has been collected by the device. To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).

(b) Contents of Order.— An order issued under this section—

(1) shall specify—

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an

order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and

(D) a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register or trap and trace device under section 3124of this title.

(c) Time Period and Extensions.—

(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed sixty days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed sixty days.

(d) Nondisclosure of Existence of Pen Register or a Trap and Trace Device.— An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that—

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line or other facility to which the pen register or a trap and trace device is attached or applied, or who is obligated by the order to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

SECTION 3124. ASSISTANCE IN INSTALLATION AND USE OF A PEN REGISTER OR A TRAP AND TRACE DEVICE

(b) Trap and Trace Device.— Upon the request of an attorney for the Government or an officer of a law enforcement agency authorized to receive the results of a trap and trace device under this chapter, a provider of a wire or electronic communication service, landlord, custodian, or other person shall install such device forthwith on the appropriate line or other facility and shall furnish such investigative or law enforcement officer all additional information, facilities and technical assistance including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such installation and assistance is directed by a court order as provided in section 3123 (b)(2) of this title. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished, pursuant to section 3123 (b) or section 3125 of this title, to the officer of a law enforcement agency, designated in the court order, at reasonable intervals during regular business hours for the duration of the order.

(d) No Cause of Action Against a Provider Disclosing Information Under This Chapter.— No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter or request pursuant to section 3125 of this title.

SECTION 3127. DEFINITIONS FOR CHAPTER

As used in this chapter—

(1) the terms "wire communication", "electronic communication", "electronic communication service", and "contents" have the meanings set forth for such terms in section 2510 of this title;

(2) the term "court of competent jurisdiction" means—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—

(i)has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located;

(iii) is in or for a district in which a landlord, custodian, or other person subject to subsections (a) or (b) of section 3124 of this title is located; or

(iv) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

(3) the term "pen register" means 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;

(4) the term "trap and trace device" means 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;

Appendix C: Select Sections of Title 50 (Foreign Intelligence Surveillance Act) as amended by the Patriot Act

U.S. CODE TITLE 50—WAR AND NATIONAL DEFENSE

CHAPTER 36—FOREIGN INTELLIGENCE SURVEILLANCE

SUBCHAPTER I—ELECTRONIC SURVEILLANCE

SECTION 1804. APPLICATION FOR COURT ORDERS

(a) Submission by Federal officer; approval of Attorney General; contents Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter. It shall include—

> (6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official
>
> > (B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

SECTION 1805. ISSUANCE OF ORDER

(c) Specifications and directions of orders

> (2) Directions An order approving an electronic surveillance under this section shall direct—
>
> > (B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, or in circumstances where the Court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier,

landlord, custodian, or other person is providing that target of electronic surveillance;

SUBCHAPTER II—PHYSICAL SEARCHES

SECTION 1823. APPLICATION FOR ORDER

(a) Submission by Federal officer; approval of Attorney General; contents
Each application for an order approving a physical search under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge of the Foreign Intelligence Surveillance Court. Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements for such application as set forth in this subchapter. Each application shall include—

(6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive branch officers employed in the area of national security or defense and appointed by the President, by and with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official—

(B) that a significant purpose of the search is to obtain foreign intelligence information;