The Security of America's Fourth Amendment Rights: A Study on National Security Letters

by

Maria Thompson

A Thesis Submitted to the Faculty of

The Wilkes Honors College

in Partial Fulfillment of the Requirements for the Degree of

Bachelor of Arts in Liberal Arts and Sciences

with a Concentration in Law and Society

Wilkes Honors College of

Florida Atlantic University

Jupiter, Florida

May, 2008

The Security of America's Fourth Amendment Rights: A Study on National Security Letters

by

Maria Thompson

This thesis was prepared under the direction of the candidate's thesis advisor, Dr. Mark Tunick, and has been approved by the members of her supervisory committee. It was submitted to the faculty of The Honors College and was accepted in partial fulfillment of the requirements for the degree of Bachelor of Arts in Liberal Arts and Sciences

SUPERVISORY COMMITTEE:

_____
Dr. Mark Tunick

_____
Dr. Martin Sweet

_____
Dr. Jeffery Buller, Dean, Wilkes Honors College

_____
Date

Acknowledgements

I would like to acknowledge Dr. Mark Tunick for the countless hours that he spent assisting me in my research and writing. It was in large part due to Dr. Tunick's tireless efforts that this thesis was completed. Dr. Tunick aided in every part of the thesis process and it was his assistance that helped me to learn far more from this experience than I could have imagined. I would also like to acknowledge Dr. Martin Sweet for his encouragement and assistance throughout my research and writing. Dr. Sweet has been a profound inspiration throughout the entirety of my collegiate experience. Dr. Sweet and Dr. Tunick have both challenged me to become a better student and their efforts have prepared me to pursue my goals.

ABSTRACT

Author	Maria Thompson
Title	The Security of America's Fourth Amendment: A Study on National Security Letters
Institution:	Wilkes Honors College at Florida Atlantic University
Thesis Advisor:	Dr. Mark Tunick
Degree:	Bachelor of Arts in Liberal Arts and Sciences
Concentration:	Law and Society
Year:	2008

National Security Letters allow the Federal Bureau of Investigation to obtain records on individuals from corporations without prior judicial intervention or approval. Statutory changes, most significantly those resulting from the passage of the United States Patriot Act in 2001, have substantially altered the four different federal statutes from which National Security Letters originate. In creating these National Security Letters the government intended to protect its citizens from national security threats. This goal has been regarded historically as legitimate, but the legislation potentially limits rights, which raises the question of whether these letters are acceptable. Drawing on relevant case law and scholarly opinion**,** I argue that use of these letters is unacceptable and may render the Fourth Amendment's protection of person and property from unreasonable searches meaningless in certain federal investigations

Dedication

To God, for without Him this would not have been possible, to my amazing family, Mom, Dad, and Hugh, and to all of my wonderful friends

Table of Contents

Introduction

The United States Government is responsible for the safety and security of its citizens, particularly during times of war and national threat. To fulfill this responsibility, the government has full access to all the necessary tools and resources to ensure the nations' safety. Following the events of September 11th, 2001, the worst attack on American soil in United States history forced the government to implement drastic regulations to aid investigations and further protect the country and its citizens. These regulations expanded governmental authority and allowed for full surveillance and investigation of individuals thought to pose a threat to national security. The most important statutory changes came with the passage of the "Uniting and Strengthening America by Providing Tools Required to Intercept and Obstruct Terrorism Act of 2001" or, as it is more commonly referred to, "The United States Patriot Act." While this act encompassed a number of enhanced security measures, I focus solely on the amendments to the existing National Security Letters and the resulting implications on the Fourth Amendment.

National Security Letters are tools that may be used by the FBI to conduct searches on individuals and corporations to gain information from a wide variety of sources without probable cause or issuance of a warrant. These letters exist in five different forms and originate from four different federal statutes.[1] Each type of letter enables the government to access different information from different specified sources. These five versions of National Security Letters vary in the type of information that may be gathered as well as the procedure for procuring this information. Despite these differences all five versions were quite substantially altered by the passage of the United States Patriot Act. The details of these five types of National Security Letters, their statutory origins, as well as the changes made by the United States Patriot Act are discussed in detail in chapter one.

1 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007.

National Security Letters have been challenged in four separate district and appellate court cases on both First and Fourth Amendment grounds. While there are aspects of National Security Letters that are inconsistent with both amendments, I focus on the Fourth Amendment claims and the importance of protecting the privacy of the information that may be accessed. According to the Fourth Amendment, citizens are protected from unreasonable searches and seizures. While what counts as unreasonable has varied based on the context of the time and the totality of circumstances, there are certain standards for a reasonable search that the Supreme Court has articulated and applied in its decisions. These standards have undergone tremendous transformation over the years. These standards and a background of the Fourth Amendment is discussed in detail in chapter two and I use chapter three to apply these standards to the FBI's use of National Security Letters.

I argue that the FBI should be required to obtain a warrant prior to issuing National Security Letters. This extra judicial scrutiny ensures that the FBI does not continue to abuse this powerful search tool and helps to ensure the privacy of American citizens. Drawing on various scholarly discussions on the right to privacy and privacy in the information age I argue its importance and show why national security does not justify violating this right. National Security is arguably one of the most important responsibilities of a government. In its role as protectorate, the United States attempts to use its power and resources to investigate individuals and prevent harm to the nation as a whole. At the same time the United States has bound itself through the constitution and several statutes to the protection of civil liberties and individual rights. These two responsibilities have clashed several times in history and often judicial and legislative determinations involve an attempt to balance them. Through a discussion of the scholarly debate and judicial precedents on privacy and national security I use chapter four to discuss this balancing act and why present use of National Security Letters tip the balance in an unacceptable way.

Drawing on scholarly opinion, judicial precedents, Congressional reports, and news reports, I argue that FBI agents should be required to obtain a search warrant prior to issuing National Security Letters, which would force them to establish probable cause and limit their ability to conduct fishing expeditions into the private lives of non-Americans and Americans alike. I argue that without the addition of a warrant requirement these letters lack the procedural safeguards necessary to protect a citizen from unreasonable searches and seizures as guaranteed by the Fourth Amendment.

Literature Review

The National Security Letter Debate

National Security Letters have been around in some form since the 1970s. They have undergone a tremendous transformation over the past several years from their meager existence as a minor foreign intelligence exception within four privacy statutes to their new status as arguably one of the most powerful intelligence tools in existence. This transformation was for the most part a direct result of the passage of the *United States Patriot Act* in 2001. Currently, the Federal Bureau of Investigation is under scrutiny by many for using their National Security Letter authority in a manner that exceeds constitutional acceptability. For this reason, National Security Letters are one of the hottest topics today and telecommunication companies, interest groups and constitutional scholars are all taking part in the discussion. Newer and more detailed information on National Security Letters is being released each month as Americans are just now being told about the FBI's extensive use and abuse of National Security Letters and the information that they allow them to obtain.

Recently, the Department of Justice's Office of the Inspector General published two reports on the FBI's use of National Security Letter authority which showed numerous errors and questionable tactics. These reports as well as the results of two cases where recipients of National Security Letters have challenged the FBI's use of National Security Letters have really brought to light the details of an investigatory tool that has been for the most part surrounded by secrecy. While most of this information has only very recently been released, several scholars have discussed the acceptability of National Security Letter searches. There exists an evident dichotomy in the literature between those who support the FBI's use of National Security Letters and those who oppose the use of National Security Letters in their current form.

Several scholars have argued that National Security Letter provisions are unacceptable while a few have argued that they are constitutionally acceptable in their current form. In arriving at their conclusions, however, each scholar's approach is unique. One reason for why these arguments are all very unique is the numerous changes that National Security Letters have undergone over the past several years. These changes, which include adding an explicit, after the fact judicial review provision, occurred sporadically over the past several years, and have affected the debate over whether National Security Letters are constitutional. For this reason various scholars had access to some information that others did not at the time of writing. There was also very limited information available on National Security Letters prior to the middle of 2007. The fact that not all of the scholars had equal access to information has provided a diversity of perspectives to the debate on National Security Letters.

One side of this debate focuses on how and why National Security Letters are unconstitutional. In the current scholarship this is the most represented side of the debate. Among the scholars that disagree with National Security Letter provisions, Zachary Shankman argues that they are vaguely worded, hinder the ability for a challenge because of the non-disclosure provision that they contain, and fail to make explicit the right to address an attorney.[2] Christopher Raab agrees with Shankman, however, he offers four different reasons for why he believes National Security Letters are unconstitutional. Raab argues that National Security Letters offer no meaningful opportunity for judicial review, the permanent gag order violates the recipient's first amendment rights, the standard for judging is unacceptably low, and the FBI's unbridled discretion increases the potential for abuse.[3] Andrew Nieland joins the position that there are problems with current National Security Letter provisions. According to Nieland, the main

2 Shankman, Zachery. Devising a Constitutional National Security Letter in light of *Doe v. Ashcroft*. The Georgetown Law Journal Vol. 94:247 (2005) p. 265 [Zachery Shankman was a J.D. candidate when he wrote this article].

3 Raab, Christopher P. Fighting Terrorism in an Electronic Age: Does the Patriot Act Unduly Compromise Our Civil Liberties? Duke Law and Technology Review Vol. 2 (2006) [Christopher Raab was a J.D. candidate when he wrote this article].

problems are the fact that they lack coherent oversight and sunset provisions, or provisions that would detail when the expanded form of National Security Letters would be reconsidered or expire.

In an attempt to address these problems, several of these scholars have offered suggestions to bring National Security Letter provisions to a level that would pass constitutional muster. According to Andrew Nieland, the problems with National Security Letter provisions are a direct result of the haphazard manner in which National Security Letter authority was expanded and the lack of knowledge on the implications of these letters. Nieland argues for Congressional correction of National Security Letter provisions. Lauren Weiner agrees with Nieland that there are problems with National Security Letters and that they must be corrected by Congress. Zachary Shankman also agrees and argues that "at minimum, a constitutional NSL process should: make explicit the right to consult an attorney; specify a process for judicial review of an NSL; allow for modification of the nondisclosure order; and require clear terminology in its authorizing statute."[4] Wiener and Nieland, however, feel that the current political climate which favors protection over civil liberties will prohibit congressional remediation of the problems. To resolve this, Nieland argues that additional oversight must come from the demands of non-governmental agencies, such as the ACLU.

When determining what changes need to be made to National Security Letters and how these changes should be made most of the scholars began by first figuring out how to classify National Security Letters under the Fourth Amendment. Lauren Weiner began her study by first determining whether National Security Letters classified as searches or seizures under the Fourth Amendment. In her study she argued that they are searches. Then she applied two Supreme Court standards for assessing the validity of warrantless searches. These standards are the

4 Shankman, Zachery. Devising a Constitutional National Security Letter in light of *Doe v. Ashcroft*. The Georgetown Law Journal Vol. 94:247 (2005) p. 265 [Zachery Shankman was a J.D. candidate when he wrote this article].

reasonableness balancing test, which states that "when the states legitimate interests outweigh the privacy interests of the individual to be searched" [5] then a warrantless search may be reasonable, and the special needs exception, which holds that "when the primary purpose of the search goes beyond the need for ordinary law enforcement and the states interest in that purpose outweighs the individuals privacy interests,"[6] a warrantless search may be reasonable. According to Weiner, National Security Letters may be constitutionally acceptable since they may potentially fit into the special categories of warrantless searches. However, she argues that this does not mean that they are without problems, which must be fixed. Others, including Zachary Shankman, are more concrete in their determinations on the constitutionality of National Security Letter provisions and go so far as to say that they are unconstitutional on many grounds.

On the other side of the debate scholars claim that National Security Letter provisions are constitutional and do not require any corrections to be acceptable. In *Unsheathing a Sharp Sword: Why National Security Letters are Permissible Under the Fourth Amendment*, Nickolas Bohl contends that there are several justifications for the government's current use of National Security Letters. According to Bohl, National Security Letters are in essence administrative subpoenas, not searches as defined under the Fourth Amendment, and as such they are acceptable under the lessened standard of reasonability, which is afforded to administrative subpoenas. Bohl argues that these letters are simply requests for information rather than searches and the FBI has the authority to issue them. For these reasons, National Security Letters are reasonable. Bohl argues that while judicial review is not prohibited by the wording of the National Security Letter provision, as argued in *Doe v. Ashcroft*, only NSL recipients, not the targets of the searches, have standing to challenge these searches on Fourth Amendment grounds. According to Bohl, Judge Marrero's claim that National Security Letters were coercive was discredited by the mere fact that

5 Weiner, Lauren. "Special" Delivery: Where do National Security Letters Fit into the Fourth Amendment. *Fordham Urban Law Journal* Vol 33 1453 – 1481 at 1463 (2006) [Lauren, Weiner was a J.D. candidate when she wrote this article].

6 Ibid.

Doe challenged his NSL. Bohl argues that the fear of National Security Letters offending privacy is simply overstated. For Bohl, there need not be any changes made to National Security Letters to make them acceptable under the constitution.[7]

How I Plan to Contribute to this Debate

Both sides of the debate present interesting perspectives in which to view National Security Letter provisions. As more information is released, the debate on whether National Security Letters are constitutionally acceptable continues. This information has given the public new insight on how the National Security Letter process works and the problems with the current procedure. All of the scholars mentioned above did not have access to this information at the time they wrote their articles. I hope to fill the gap in the current scholarship on National Security Letters by providing a study on National Security Letter use in light of new information and using this information to support my argument that National Security Letters are unconstitutional on Fourth Amendment grounds.

7 Bohl, Nickolas J. Unsheathing a Sharp Sword: Why National Security Letters are Permissible Under the Fourth Amendment [Note] Boston University Law Review Vol. 86 (2006) [Nickolas Bohl was a J.D. candidate when he wrote this article].

Chapter 1: National Security Letters

1.0 Introduction

The purpose of this chapter is to explain what current government practice and law is concerning the use of National Security Letters. This chapter provides a background on National Security Letters, the origins of the four statutes with National Security Letter provisions and the adaptations and alterations they have undergone over time. I focus on the changes made by the *United States Patriot Act* and the effect of these changes on the Federal Bureau of Investigation's use of these letters. I also discuss the changes that have resulted through pre and post Patriot Act legislation and the effect of several district court rulings on the applicability of the current National Security Letter provisions. I conclude this chapter with a discussion on the two reports published by the Office of the Inspector General regarding the FBI's use of National Security Letters and the new Telecommunication bill recently passed by Congress.

1.1 Origins

A National Security Letter (NSL) is an investigatory tool granted to the Federal Bureau of Investigation (FBI) through federal statutes enacted during the 1970s and 1980s. These letters were originally created as exceptions to various privacy acts to better enable the FBI to conduct investigations of foreign agents and powers. They allow the FBI to gain access to certain information without prior judicial intervention or approval. In order to issue these letters FBI field officers are required to gain permission and approval from within the bureau itself. These letters are never taken before a judge or even an impartial authority outside of the FBI prior to their delivery to the recipient. In fact, these letters never face judicial scrutiny at any point in the process of approval, delivery, or upon receipt of information.[8]

There are five different forms of National Security Letters as delineated by four separate statutes within the United States Code. Each NSL provision is unique. However, several common

8 The lack of judicial scrutiny was discussed in the district court case *Doe v. Ashcroft*, discussed in Chapter Two. The court referred to the FBI's use of NSLs as failing to provide proper judicial scrutiny or at least failing to make it so that a reasonable person would feel that a right to such scrutiny existed.

threads exist within all five forms. National Security Letters, regardless of their originating statute--with the exception of those stemming from the National Security Act--allow the FBI to access information upon a self certification that the information is

> Relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.[9]

Each statute containing an NSL provision enables the FBI to obtain information from different, specified sources to aid in their investigations. Each National Security Letter provision has slightly different requirements and standards for the National Security Letters it permits and describes what type of information may be retrieved. The four statutes that include NSL provisions are: The Right to Financial Privacy Act (RFPA), Electronic Communication Privacy Act (ECPA), Fair Credit Reporting Act (FCRA), and National Security Act.

The Right to Financial Privacy Act (RFPA) was the first act to contain a National Security Letter provision. This act was designed to "protect the customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity."[10] The RFPA guarantees that "federal agencies would provide individuals with advance notice of requested disclosures of personal financial information and affords individuals an opportunity to challenge the request before disclosure is made to law enforcement authorities."[11] The National Security Letter provision of the RFPA was enacted in 1986 and it established that the FBI may be exempted from the advance notice requirement when obtaining financial information in foreign counter-intelligence cases.

9 United States Patriot Act U.S. H.R. 3162, Public Law 107-56 Title v. §505.

10 Right to Financial Privacy Act H.R. Rep. No. 95-1383 (1978) at 133.

11 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007.at 12.

The RFPA National Security Letter provision allows the FBI to obtain "information regarding open and closed checking and savings accounts and safety deposit box records."[12] This information may be requested from "banks, credit unions, thrift institutions, investment banks or investment companies. Transactions with issuers of traveler's checks, operators of credit card systems, pawnbrokers, loan or finance companies, travel agencies, real estate companies, casinos, and other entities may also be obtained with these letters."[13]

The Electronic Communication Privacy Act (ECPA) differs from the RFPA in the information that it protects.[14] This act was created to protect electronic and wire communications retained by third parties.[15] Typically these third parties are referred to as Internet Service Providers or ISP's. The statute does not further explain what entities can be classified as an ISP. In fact, the FBI has classified several diverse businesses, and locations as internet service providers including libraries.[16] The National Security Letter provision within the ECPA allows FBI agents to request "subscriber information and toll billing records or electronic communication transactional records" from "wire or electronic communications service providers" to aid in foreign counterintelligence investigations."[17]

This provision allows the FBI to collect historical information on telephone calls made from a specified number, including land lines, cellular phones, prepaid phone card calls, toll free calls, alternate billed number calls (calls billed to third parties), and local and long distance billing records associated with the phone numbers (a.k.a. toll records); "Electronic communication transactional records include: e-mail addresses associated with the account; screen names; billing

12 Ibid., at xii.

13 Ibid., at 13.

14 Electronic Communications Privacy Act 18 U.S.C. § 2709 (1988).

15 Ibid., at 13.

16 This qualification was challenged in the United States district court in *Doe v. Gonzales* 386 F.Supp.2d 66 D. Conn., (2005) [decision later rendered moot].

17 Ibid., at 13.

records and method of payment."[18] The FBI may also obtain subscriber information associated with particular telephone numbers or e-mail addresses, such as their name, address, length of service, and method of payment."[19] This statute has also been construed to allow FBI agents to obtain an individual's web activity history, including a history of all websites visited and all online searches conducted. Numerous articles in the *New York Times* and the *Washington Post* as well as reports and arguments posed by various interest groups claim that the NSL provisions, which contain numerous undefined terms, such as ISP, electronic communication records, toll billing information…etc, have enabled the FBI to access these records.[20]

The Fair Credit Reporting Act (FCRA) was designed to protect "personal information collected by credit reporting agencies."[21] The FCRA NSL provision, enacted in 1996, enabled the FBI to gather certain, limited information regarding an individual's credit history through these National Security Letters. This information includes: the names and addresses of all financial institutions at which a consumer maintains or has maintained an account; and consumer identifying information limited to the name, current address, former addresses, places of employment, or former places of employment pursuant to FCRAu NSLs."[22] In 2001, an additional NSL provision was added to the FCRA. This new provision is discussed later in this chapter.

The National Security Act (NSA), enacted in 1947, is an act protecting information stored on government officials. In 1994, Congress amended the NSA to include a National Security Letter provision. This provision enables the FBI to access information stored on certain current and potential government employees. This amendment occurred in light of the events surrounding the

18 Ibid., at 13.

19 Ibid., at 13.

20 Barton, Gellman. ""The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans." The Washington Post, November 6, 2005. at AO1.

21 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007at 14.

22 Ibid.

espionage investigation of former Central Intelligence Agency Agent Aldrich Ames.[23] The National Security Letter provision of this statute is unique as it is only applicable to current or former employees of the executive branch of the United States who have access to classified information.

Originally, FBI agents had to ensure that "there are specific and articulable facts giving reason to believe that the person or entity to which the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978."[24] Currently, the FBI no longer has to ensure the existence of a foreign nexus. They must now ensure a much lesser standard which I further discuss later in this chapter. This very controversial and important change occurred as a direct result of the passage of the United States Patriot Act in 2001.

1.2 Principle Objectives of National Security Letters

The FBI has argued that NSLs are vital in their national security investigations. In fact, according to the Inspector General's Report to the Department of Justice some FBI agents have gone so far as to liken National Security Letters to their "bread and butter."[25] In this report the FBI provided numerous reasons as to why NSLs are vital to their investigations. Their primary claim was the speed and efficiency that NSLs provide as a means of data collection.[26] In a recent press release the FBI made the following comment regarding National Security Letters:

> In the post 9/11 world, the National Security Letter is an indispensable tool and building block of an investigation that contributes significantly to the FBI's ability to carry out its national security responsibilities by directly supporting the furtherance of the counterterrorism, counterintelligence and intelligence missions.[27]

23 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007at 14.

24 Electronic Communications Privacy Act Title 18 U.S.C. § 2709 (1986).

25 Ibid.

26 Ibid.

27 FBI Press Release http://www.fbi.gov/pressrel/pressrel07/nsl_faqs030907.htm date accessed December 1st 2007.

The FBI uses the information that they gain from National Security Letter searches to provide evidentiary support for FISA applications for electronic surveillance, physical searches, pen register orders, and trap and trace orders.[28] A second use they have for these letters is to find links between those under investigation and those in contact with these suspects. They use the information gained from the various statutes to study both financial and communication links. This investigation technique is called "link analysis."[29] NSLs are used as a preliminary step in building a national security investigation. National Security Letters enable the FBI to use the information that they obtain and any links they find to help other field divisions, the joint terrorism task forces, federal agencies and foreign governments develop cases and investigations. They also disseminate the "analytical products" that they develop with this information to various members of the intelligence community including other federal agencies and within the FBI and other departments.[30] The FBI also uses this information to aid in criminal proceedings by disseminating the information they receive to law enforcement authorities and the District Attorney's Office.

The FBI argues that the information they gather is beneficial in their process of limiting their suspects in national security investigations by allowing them to collect sufficient information to eliminate their concerns about a number of suspects and close those cases. Finally, they argue that these letters are helpful because they can help to corroborate evidence and information gained from various other investigative tools and techniques within their power.[31]

1.3 Amendments

National Security Letter provisions have been altered tremendously since their enactments under the above mentioned sections of the United States Code. Through various Congressional

28 FISA stands for the Foreign Intelligence Surveillance Act. This act details the types of investigations that may be conducted on certain foreign nationals and creates a court where cases involving foreign nationals may be heard.

29 Barton, Gellman. ""The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans." The Washington Post, November 6, 2005. at AO1.

30 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007 at xxii.

31 Ibid.

actions the statutes governing National Security Letters have become far more powerful. In their current state, NSLs can be used to access information about foreign powers and agents of foreign powers as well as information about United States citizens. NSLs have transformed from mere unenforceable requests for information to now mandated information requests under threat of fine or penalty of law.[32]

All of the four original National Security Letter provisions have been altered by various acts of Congress prior to the Patriot Act. As mentioned, one change that occurred was the Congressional decision in 1986 to allow the FBI to make compliance with these National Security Letters mandatory under penalty of law.[33] This change came with minor alterations limiting the scope of the statutes and had a direct impact on both the Right to Financial Privacy Act and The Electronic Communication act. Arguably, the most prominent and important change occurred to the National Security Letter provision of the Electronic Communication Privacy Act in 1993 when the Senate Judiciary decided that the FBI should have the authority to use National Security Letters to target United States citizens who contact or are connected to foreign powers or agents of foreign powers.[34] This differed vastly from the original statute which required that the target of the investigation must be a foreign power or an agent of a foreign power. While the revised statute still required a connection to a foreign power, the change allowed for certain U.S. citizens to be targeted. This change was later applied to all other NSL provisions.

1.4 Patriot Act

The most noteworthy changes to the FBI's authority to use National Security Letters and the information that they can request resulted from the passage of the "The United States Patriot Act." This act drastically revised several existing federal statutes, regarding agencies and instruments used in federal and international investigations. However, I focus solely on the

32 These changes were listed in the legislative history section of the decision in *Doe v. Ashcroft* 334 F.Supp.2d 471 S.D.N.Y. 2004.September 28, 2004 at 500.

33 Ibid.

34 Ibid.

changes made to the four federal statutes containing National Security Letter provisions as well as the additional National Security Letter provision this act created.

The Patriot Act made several alterations to the text of the four National Security Letter provisions. These changes included establishing a looser standard required for a National Security Letter to be issued. Under this new standard for an FBI agent to issue a National Security Letter they must prove that the information sought is:

> Relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.[35]

This standard, which no longer required any connection to a foreign agent or power, enabled the FBI to target Americans, as well as individuals not directly under investigation by the FBI with NSLs. This differed from the original standard which required that National Security Letters may only be issued if there is a proven existence of a connection, albeit minimal, to a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act. [36] By completely removing any required nexus to foreign agents or powers the FBI was empowered to conduct searches on a much wider population of individuals.

Following these changes, an FBI agent can use one or multiple National Security Letters to request information on American citizens whom their investigations target as well as information on any individual who comes into contact with these citizens. For example, if the FBI is investigating person A, who for the purposes of this example is an American citizen, and person A has 30 people in his phone or email contact list, the FBI can use one or more National Security Letters to get not only the information on person A but they may request information on each of the individuals on person A's phone/email contact list. This expansion of power was

35 United States Patriot Act U.S. H.R. 3162, Public Law 107-56 Title V §505.

36 While this nexus was already lessened by the 1993 Congressional revision of the ECPA, the Patriot Act fully removed the requirement that an individual targeted by a NSL must be linked in some way to a foreign agent or power.

made quite evident by the spike in the FBI's use of these letters to a point nearly five times that of the pre-Patriot Act period.[37]

The effects of the above mentioned change were intensified by a Patriot Act amendment that increased the number of FBI officials that are able to approve the use of NSLs. Prior to the Patriot Act the only officials within the FBI that were able to approve the use of a National Security Letter were the Director or his appointee no lower than Deputy Assistant at FBI headquarters.[38] The Patriot Act lessened this requirement by empowering special agents at FBI field offices to issue NSLs.[39] This change was important, because it allowed the FBI to use the lessened required standard to the fullest extent.

Even though NSLs may now be used to target American citizens the FBI was not required to change the procedure they follow to issue them. NSLs are now, arguably, the most powerful investigatory tool available to target United States citizens. This is disturbing as there is no judicial intervention or review prior to the issuance of an NSL in an investigation

While the above mentioned changes effected every NSL provision, with the sole exception of the NSA NSL provision, there were also important, additional, and specific changes made to the Fair Credit Reporting Act. The Patriot Act created a new FCRA NSL provision. This new provision is the most expansive NSL provision as it allows the FBI to gather all financial information on the target of their investigation. The new provision was for an FCRAv National Security Letter that "authorized the FBI to obtain full credit reports on individuals during national security investigations."[40] This particular provision allows the FBI to access more information than any other NSL provision existing within the original four statutes. The text of the statute

37 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007. at xviii.

38 Barton, Gellman. ""The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans." The Washington Post, November 6, 2005. at AO1.

39 2001 Amendments Subsection (b) Pub.L. 107-56, § 505(a) (1), in the matter preceding paragraph (1), inserted "at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director" after "Assistant Director."

40 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007. at 14.

requires the recipient to provide the FBI with all information within their files on the individual being investigated.[41]

The NSL provision of the National Security Act is substantially different than the other five National Security Letter provisions and for this reason it was not altered to the extent of the others. The targets of these letters are limited to certain current or former employees of the federal government. The NSA NSL authorizes the FBI to collect information on certain U.S. Citizens, in specific circumstances, even before the passage of the United States Patriot Act. The only changes that have been made to this act occurred as a result of the Reauthorization Act of 2006 which ensured that judicial review is made explicitly available to recipients prior to penalization for non-compliance.

The many amendments to the NSL provisions led to dramatic and rapid changes in the FBI's use of these letters. These changes are evidenced by the Office of the Inspector General's findings in his report to the Department of Justice on the FBI's use of these letters. This report, which I discuss in further detail later in the chapter, discussed the increasing number of National Security Letters being issued as well as numerous errors that he found when examining how the FBI uses these letters. The original report, released March 2007, along with a new updated report, released in March 2008, stated that the FBI has made drastic changes to its National Security Letter procedure. Numerous problems still exist however, and require further correction. The problems that exist in the FBI's use of NSLs have also been addressed by courts following challenges made by interest groups and certain NSL recipients.

1.5 Cases regarding National Security Letters: Rulings and Implications

There have been four cases regarding National Security Letters: *Doe v. Ashcroft* (2004, *Doe v. Gonzales* I (2005), *Doe v. Gonzales* II (2006), and *Doe v. Gonzales* III (2007). Three of these cases were heard at the district court level --*Doe v. Ashcroft*, *Doe v. Gonzales* I (2005), and

41 (15 U.S.C.A. § 1681v (a) "a consumer reporting agency shall furnish a consumer report of a consumer and all other information in a consumer's file").

Doe v. Gonzales III (2007) -- and one of the cases, *Doe v. Gonzales* II (2006), was heard by an appellate court. These cases regarded constitutional challenges to National Security Letter provisions on both First Amendment and Fourth Amendment grounds. While the majority of these cases focused solely on the First Amendment claims, I focus on *Doe v. Ashcroft*, which discussed Fourth Amendment claims brought by the ACLU, and *Doe v. Gonzales*, (2007), which discussed the effect of the Patriot Act Reauthorization on the original Fourth Amendment claims made in *Doe v. Ashcroft*. I only briefly discuss the First Amendment claims addressed in the four cases while noting that it was these claims that had the greatest impact in these cases. The cases described below all involve legal challenges to the FBI's use of National Security Letters pursuant to the National Security Letter provision of the Electronic Communications Privacy Act.

1.51 *Doe v. Ashcroft*

Doe v. Ashcroft, the first case ever heard regarding the FBI's use of National Security Letters, was decided in the Southern District Court of New York on September 28th, 2004. In this case Judge Marrero discussed the Fourth Amendment claims brought by the complainant John Doe, real identity not revealed, as well as the First Amendment claims, which I briefly discuss later in the chapter. In addressing the challenge to NSLs on Fourth Amendment grounds Judge Marrero held that "the compulsory, secret, and unreviewable production of information required by the FBI's application of 18 U.S.C. §2709 violates the Fourth Amendment."[42]

Judge Marrero based a portion of his argument on the Fourth Amendment claims brought by the complainant however, he decided not to address the complainants request for a facial invalidation of §2709 on Fourth Amendment grounds. Judge Marrero gave two reasons for ruling on the Fourth Amendment claims as an as applied challenge over a facial invalidation: first, he claimed that "even if the court accepted the government's interpretation of the statute, which included an implicit ability by an ISP to challenge the NSL, the court would not be addressing the plaintiffs claim that in practice §2709 in all or a vast majority of actual cases, by virtue of the

42 *Doe v. Ashcroft* 334 F.Supp.2d 471 S.D.N.Y. (2004). at 525.

statute's unwarranted application by the FBI operates otherwise" and second, "there has been no evidence that NSLs have ever been challenged prior to this case, making it less likely that a reasonable individual would feel the right to challenge them."[43] In his decision, Judge Marrero looked at similar investigatory tools and the statutes that create them, in particular those concerning administrative subpoenas, pen traps, wire traps, and grand jury subpoenas concluding that

> NSLs such as the ones authorized by §2709 provide fewer procedural protections to the recipient than any other information gathering technique the government employs to procure information similar to that which it obtains pursuant to §2709.[44]

Judge Marrero also differentiated National Security Letters in light of the non-disclosure provision that they contain. In doing so he argued:

> The form NSL, which is proceeded by a personal call from an FBI agent, is framed in imposing language on FBI letterhead and which, citing the authorizing statute, orders a combination of disclosure in person and in complete secrecy, essentially coerces the reasonable recipient into immediate compliance. Objectively viewed, it is improbable that an FBI summons invoking the authority of a certified "investigation to protect against international terrorism or clandestine intelligence activities," and phrased in tones sounding virtually as biblical commandments, would not be perceived with some apprehension by an ordinary person and therefore elicit passive obedience from a reasonable NSL recipient.[45]

Based on this reasoning Judge Marrero argued that "it is highly unlikely that an NSL recipient reasonably would know that he may have a right to contest an NSL through a judicial proceeding."[46] To justify this claim, Judge Marrero cited evidence that prior to this case there had never before been a challenge to an NSL provision despite the fact that NSLs have been around

43 *Doe v. Ashcroft* 334 F.Supp.2d 471 S.D.N.Y. (2004). at 501-502.

44 Ibid., at 484.

45 Ibid., at 501.

46 Ibid.

since 1978.[47] Judge Marrero argued that "in testing the validity of a government policy or law," one must, "recognize the importance of appreciating its practical effect on a reasonable person."[48]

Judge Marrero argued that the lack of Fourth Amendment procedural protections intensified the non-disclosure provision which implicates an individual's First Amendment rights. The fact that the government may use these letters to access information that is protected by the First Amendment provides even more justification that they should explicitly require the judicial review which the government argues implicitly exists. These letters can potentially give the FBI access to things such as political campaign members and supporters, and the anonymous identity of those whose online web blogs are viewed as troubling, even though this information may be barred by the stipulation that the FBI cannot conduct searches based solely on First Amendment activity. According to Judge Marrero, "These prospects only highlight the potential danger of the FBI's self-certification process and the absence of judicial oversight."[49]

Judge Marrero noted in his decision the specific terms within the ECPA NSL provision by claiming that "the statutes' reference to "transactional records creates ambiguity regarding the scope of the information required to be produced by the NSL recipient."[50] This ambiguity is worsened by the statement in the NSL which "asks the recipient to provide the government with any other information which they consider to be an electronic communication transactional record

47 Marrero cited both the Department of Justice's report to the House Judiciary Committee in 2003 which stated that "there had been no challenges to the propriety or legality of any NSLs and the Governments evidence in the case which Marrero claimed conspicuously lacks any suggestion either that the Government has ever had to resort to a judicial enforcement proceeding for any NSL or that any recipient has ever resisted an NSL request in such a proceeding or via any motion to quash". In addition, "the evidence suggests that perhaps even the FBI does not actually believe that § 2709 contemplates judicial review first, based on a senior FBI agents testimony before Congress that there was no judicial enforcement provision in 2709 [H.R. 3179 Hg statement of Thomas J. Harrington Deputy Assistant Director, FBI] and second, plaintiffs have obtained, via a FOIA request, two FBI memoranda disturbing implementing and serving NSLs, yet neither memorandum discusses or even mentions the possibility that an NSL recipient could challenge the NSL in court." (Ibid., at 502 and FN 146).

48 *Doe v. Ashcroft* 334 F.Supp.2d 471 S.D.N.Y. (2004). at 503 citing *Bantam Books, Inc v. Sullivan* 372 U.S. 58 (1963).

49 Ibid., at 507.

50 Ibid.

in addition to information that §2709 specifically authorizes the FBI to collect."[51] For as Judge Marrero states:

> The practical absence of judicial review may lead ISP's to disclose information that is protected from disclosure by the NSL itself, such as in a case where the NSL was initiated solely in retaliation for the subscriber's exercise of his First Amendment rights as prohibited by §2709(b)(1)-(b)(2). Only a court would be able to definitively construe the statutory and First Amendment rights at issue in the "First Amendment retaliation" provision of the statute, and to strike a proper balance among those interests.

Judge Marrero argued that the Supreme Court precedents limiting a subscriber's Fourth Amendment claims over information given to a third party have a different meaning in the context of the internet. Marrero argues, "no court has adopted the Government's argument that anonymous internet speech or associational activity ceases to be protected because a third-party ISP is in possession of the identifying information."[52] Judge Marrero claimed that "the Court is persuaded that, for First Amendment purposes, internet records of the type obtained via a §2709 NSL could differ substantially from transactional bank or phone records."[53] Even though Judge Marrero argued this point on First Amendment grounds this justification could apply to a Fourth Amendment challenge as well.

Drawing support from the important Fourth Amendment precedent *Katz v. United States*, further discussed in the following chapter, Marrero argued:

> A person who signs onto an anonymous forum under a pseudonym, for example, is essentially "shutting the door behind him" and is surely entitled to a reasonable expectation that his speech, whatever form the expression assumes, will not be accessible to the Government to be broadcast to the world absent appropriate

51 Ibid., at FN 168.

52 *Doe v. Ashcroft* 334 F.Supp.2d 471 S.D.N.Y. (2004).at 508 Justice Marrero prefaced this information in Footnote 171 by citing precedents indicating that internet users have no Fourth Amendment right to prohibit disclosure of information they have voluntarily turned over to ISP and cited *Guest v. Leis* 255 F.3d 325, 336 (6th Cir.2001) which held that plaintiffs…lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the systems operators and also cited *United States v. Kennedy* which held that defendant could not "claim to have a Fourth Amendment privacy interest in his subscriber information" because when defendant entered into an agreement with Road Runner for Internet service, he knowing[ly] revealed" the information to his ISP.

53 Ibid., at 509.

> legal process. To hold otherwise would ignore the role of the internet as a remarkably powerful forum for private communication and association, a role that even the government concedes.[54]

Judge Marrero's decision to liken signing on to a website to shutting a door behind you in a phone booth could arguably imply his belief that an individual has both a reasonable expectation that his speech will not be invaded, as he argues, and a reasonable expectation of privacy in this realm as well. I justify this by making note of the case that Judge Marrero cites, *Katz v. United States*, which uses the idea of shutting the door behind you to implicate an individual's privacy rights in a phone booth. If, as Marrero argues, signing on to a web page is the same as shutting the door behind you, that would appear to mean that by entering in a user name and password one is entitled to the same reasonable expectation of privacy in that information.

In his decision Judge Marrero states that the court knows that the internet may be used for criminal activity and that there are certainly circumstances where the First Amendment would be forced to yield to a compelling interest of government to obtain the records of internet firms. Despite this, certain fundamental rights are implicated in cases in which the government broadly interprets §2709. For this reason, judicial review is an important safeguard to "ensure that if an infringement of those rights is asserted, they are adequately protected through fair process in an independent neutral tribunal."[55]

In determining the level of scrutiny which should be applied during the judicial review of National Security Letters Judge Marrero focused on the threat to an individual's First Amendment protections under § 2709. Judge Marrero argued that speech restrictions which are either content based or impose a prior restraint on speech are presumed invalid and may be

54 The Supreme Court ruled in this case that "the government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a search and seizure within the meaning of the Fourth Amendment." The Supreme Court also held that "a person entering a phone booth who shuts the door behind him is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world" and "to read the constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

55 *Doe v. Ashcroft* 334 F.Supp.2d 471 S.D.N.Y. (2004).at 511.

upheld only if they are "narrowly tailored to promote a compelling government interest." This standard mandates that if less obtrusive means are available the statute is not narrowly tailored and runs the risk of invalidation. Because §2709c implicates First Amendment protections the court agreed with the plaintiff that these letters should be subject to strict scrutiny.[56] By using strict scrutiny to resolve the complainant's First Amendment challenge, Judge Marrero decided to facially invalidate the ECPA NSL provision. Due to the implications of the ruling and the importance of the issues involved, the holding was stayed for ninety days to give the government appropriate time to appeal the result.[57] This decision was later vacated by *Doe v. Gonzales* (2007).

1.52 Doe v. Gonzales (Doe II) (2005)

In 2005, the District court of Connecticut heard a different but similar case regarding National Security Letters. This case is referred to as *Doe v. Gonzales* or Doe II.[58] In this case the complainant, Mr. George Rice, the head of library connections, which manages a group of libraries in Connecticut, challenged his receipt of a National Security Letter. Mr. Rice claimed the NSL issued to him under the ECPA National Security Letter provision was unconstitutional on First, Fourth, and Fifth Amendment grounds. In his decision, Judge Hall focused on the First Amendment claims surrounding the non-disclosure provision and did not address the contention that this provision violated the complainants Fourth and Fifth Amendment rights. The resulting holding was that the ECPA NSL provision was facially unconstitutional on First Amendment grounds as it failed to meet the standards of strict scrutiny. Judge Hall also chose to stay his ordered injunction on the FBI's use of this type of National Security Letter to leave the government time to appeal.

1.53 Doe v. Gonzales (2006)

56 Ibid., at 511-512.

57 Ibid., at 526.

58 *Doe v. Gonzales* 386 F.Supp.2d 66 D. Conn., (2005).

In 2006 both *Doe v. Ashcroft* (Doe I) and *Doe v. Gonzales* (Doe II) were brought up for appeal in the case *Doe v. Gonzales*.[59] This case was heard in the Court of Appeals in New York. In this case the appellate court looked at the two prior cases in light of the passage of the Reauthorization Act of 2006.[60] The enactment of this statute led the complainants from *Doe v. Ashcroft* to drop their Fourth Amendment claims on the grounds that the new statute explicitly guaranteed a form of judicial review for National Security Letter recipients prior to the government's ability to enforce compliance. The court of appeals argued that this decision rendered moot the portion of Judge Marrero's opinion which held that National Security Letters were unconstitutional under the Fourth Amendment. The court of appeals argued that there were new novel First Amendment claims that were created by the Reauthorization Act. The major differences in the claims now before the court and those argued in *Doe v. Ashcroft* led the court of appeals to vacate the holding in *Doe v. Ashcroft* and remand the case back to the district court for further proceedings on the new First Amendment claims.

The court of appeals then determined the standing of the decision rendered in *Doe v. Gonzales*. In this matter the court discussed the government's decision to permit the internet service provider, who challenged the ECPA NSL in Doe II, to disclose its identity as a recipient of an NSL. The court of appeals argued that this concession rendered *Doe v. Gonzales* moot because the main contention was the non-disclosure provision. This case was not remanded to the district court because there were no new claims presented.

1.54 Doe II v. Gonzales (2007)

59 *Doe v. Gonzales* 449 F.3d 413 C.A. 2 (N.Y.) (2006).

60 USA Patriot Improvement and Reauthorization Act of 2005 Pub.L. No.109-177,120 Stat. 192 (March 9th, 2006) more commonly referred to as the Reauthorization Act. This act explicitly stated that individuals who receive a National Security Letter are able to discuss their receipt with an attorney prior to compliance. This provision was codified in Title 18 of the United States Code at section 3511.

The most recent case regarding National Security Letters was *Doe II v. Gonzales*, which was heard in the Southern District of New York on September 6th, 2007.[61] One of the two main claims before the court involved the new novel First Amendment claims that the Court of Appeals felt were created by the Reauthorization Act and remanded for district court determination. These new claims involved the standard of review for the non-disclosure provision of the National Security Letter provisions in light of the required First Amendment standards of review. The second claim was a challenge of the constitutionality of the remaining standards of judicial review for National Security Letters as they are stated in section 3511 of Title 18 of the United States Code.

In his decision Judge Marrero argued that the newly created standard of review for the non-disclosure provision of National Security Letters was not tailored in a way as to ensure the standard of strict scrutiny which such profound First Amendment claims would require. Judge Marrero argued that for this reason Title 18 §3511(b), which established a very minimal standard of review for determining the validity of a non-disclosure order, was unconstitutional on First Amendment grounds. Judge Marrero's overall determination on this issue was that the revised non-disclosure provision that prevented recipients from disclosing National Security Letter receipt was unconstitutional on its face and was unseverable from the remainder of the National Security Letter provision of the ECPA codified at 18 U.S.C. § 2709.

Judge Marrero argued that the fact that the remaining sections of Title 18 §3511 implicated judicial review provisions that were fundamentally tied to the remaining four National Security Letter provisions, which have not yet been challenged, meant that his decision to not rule on the constitutionality of these sections was justified. Following this decision Judge Marrero argued that §3511(b) was severable from the remainder of §3511 and that Title 18 §3511(a) and(c) still remain valid law. In rendering this decision Judge Marrero drew heavily on the report published by the Office of the Inspector general which I discuss in detail later in the chapter.

61 *Doe II v. Gonzales* 500 F.Supp.2d 379 S.D.N.Y (2007).

As a result of the Court's decision to invalidate the non-disclosure provision of the ECPA National Security Letter provision the recipients of the National Security Letters in the above mentioned cases are the only individuals that are able to discuss receipt of a NSL. Overall the First Amendment claims surrounding the non-disclosure provision were the most significant in the holdings in all four of the above mentioned cases. The Fourth Amendment claims were never fully resolved as the complainants dropped their claims following the passage of the Reauthorization Act of 2006.[62] The fact that the Fourth Amendment claims were dropped does not necessarily mean that there remain no Fourth Amendment challenges that could be brought against National Security Letters. It simply means that any Fourth Amendment claims that may exist have not been resolved and will not be resolved until challenged. The judicial review that is explicitly made available through this statute has never been evaluated on Fourth Amendment grounds. This was a result of both the complainants' decision in the above mentioned cases to drop their Fourth Amendment claims and Judge Marrero's refusal to address any potential Fourth Amendment claims under §3511 because of its ties to the four unchallenged NSL provisions.

In both *Doe v. Gonzales* III and *Doe v. Ashcroft* Judge Marrero focused on the First Amendment grounds for invalidating the ECPA NSL, However, Judge Marrero argued his point in such a way as to arguably leave the door wide open for a Fourth Amendment challenge of these National Security Letters. Judge Marrero's opinion leaves open the question of whether an individual whose information was obtained through an NSL search could have standing to challenge an NSL rather than the ISP who actually receives the letter. Judge Marrero's decision to distinguish National Security Letters from all other investigative tools as well as the types of searches that involve third party involvement, something that usually would hinder an individual's privacy claim according to the Supreme Court, makes it plausible that an individual could successfully challenge the letters on Fourth Amendment grounds. I argue that an individual

62 USA Patriot Improvement and Reauthorization Act of 2005 Pub.L. No.109-177,120 Stat. 192 (March 9th, 2006) more commonly referred to as the Reauthorization Act.

should have the right to challenge an NSL search of their records because it would be their privacy that is invaded to a far greater extent than the ISP's privacy.

I will discuss, in chapters three and four, a potential case where this individualized challenge to an NSL could occur. In my argument I focus on precedent surrounding Fourth Amendment privacy claims over information held by third parties and I attempt to distinguish the reasoning used in these cases to argue why the information provided to these third parties should be considered to be that in which an individual has a reasonable expectation of privacy, at least in most cases. I argue that the scope and breadth of National Security Letters should justify an individual's challenge to National Security Letter searches on Fourth Amendment privacy grounds.

In the following chapter I appeal to the Fourth Amendment to justify my argument that these letters are unconstitutional in their current state. I also attempt to differentiate these particular investigatory tools from other tools that remain in the possession of the federal government and the reasons why these differences call for more stringent procedural safeguards then those stipulated by the National Security Letter provisions themselves and in Title 18 U.S.C. § 3511.

1.6 Report on the FBI's Use of National Security Letters

The USA Patriot Improvement and Reauthorization Act of 2006 a.k.a the "Patriot Act Reauthorization Act" included a Congressional directive that the Department of Justice's Office of the Inspector General must review the use, and effectiveness of NSLs issued by the FBI, including any improper or illegal use."[63] The first of these reports was to be given to Congress on March 9th 2007 and to cover calendar years 2003 -2004 and the second report was to be given to Congress on December 31st 2007 and was to cover calendar years 2005 – 2006. These reports were completed, submitted to Congress, and subsequently released to be public following declassification proceedings.

63 USA Patriot Improvement and reauthorization Act of 2005 Pub. L. No. 109-177 §119.

In the first of these two reports which was released to the public in late March 2007 the Inspector General stated numerous problems that he found with nearly every aspect of National Security Letter usage from the approval stage to the way that the information is received, stored, and disseminated. The Inspector General's report detailed numerous errors both on behalf of the FBI as well as the recipients of these letters.

In his discussion he articulated the vast effect that the Patriot Act had on the number of National Security Letters issued. According to his audit, the FBI's use of NSLs increased from 8,500 requests issued in 2000 to approximately 39,000 in 2003, 56,000 in 2004 and approximately 47,000 in 2005.[64] According to the Inspector General, the FBI's use of NSLs has been on a continuing upward trend since the passage of the Patriot Act, with the exception of nine National Security Letters containing approximately 11,100 requests under the ECPA NSL provision in 2004 that resulted in a spike in the number of requests.[65] According to his second report this trend continued in 2006 with a total of 49,425 NSLs being issued.[66] Another consistent trend that was found is the shift in the percentage of NSL requests generated from investigations on non-U.S. persons to those generated from investigations on U.S. persons. In 2003 approximately 39% of NSLs were generated in investigations on U.S. Persons this increased to approximately 53% in 2005 and finally to 57% in 2006.[67] According to the Inspector General, the number of NSLs used to investigate non-Americans has declined from 10,232 in 2003 to 8,605 in 2006 whereas searches on Americans increased from 6,519 in 2003 to 11,517 in 2006.[68]

Since NSLs are now being used more often in cases involving American citizens the numerous problems that the Inspector General notes in his report are even more disturbing. One

64Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007. at xvi.

65 Ibid. footnote number 22 at page xviii.

66 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2008 at 110.

67 Ibid. 111 and ,Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters", edited by United States Department of Justice, 2007 at xx.

68 Ibid., at 112.

of these problems was the use of inaccurate filing systems, which often resulted in inaccurately low representations of the numbers of NSLs issued. In fact, the Inspector General notes in his report "although we found that the data in the OGC database is not fully accurate or complete and overall significantly understates the number of FBI NSL requests; it is the only database that compiles information on the FBI's use of NSLS." [69] For this reason, he claims the numbers he presents may be inaccurately low. An additional problem that resulted in inaccuracies in the FBI's storage of their NSL data stemmed from the FBI's new ability to "obtain records on the contacts of a suspect, so long as the information is relevant to an authorized investigation." Apparently, the FBI does not store information on whether the target of an NSL issued during an investigation is the main suspect in the investigation or another person.

> Because the target of an NSL is frequently not the same person as the subject of the underlying investigation, the FBI does not know and cannot estimate the number of NSL requests relating to persons who are not investigative subjects.[70]

This problem was corrected in 2006 by a policy change which requires the FBI to make note of NSL requests issued for individuals other than the subject of the investigation. This new requirement ensures that the FBI also notes whether the individuals targeted in an NSL investigation are Americans or non-Americans.[71]

The problems with the filing and storage of NSL obtained data were not the only problems that the Inspector General found. In his report he noted that between 2003 and 2005 the FBI reported 26 possible Intelligence Oversight Board violations yet, during his audit he found an additional 22 possible IOB violations within a sample of only 77 investigative files stored in four field offices that had not been reported.[72] Of the 26 reported violations three involved NSLs issued in investigations that had not been appropriately approved, four involved NSLs that failed

69 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007. at xviii.

70 Ibid., at xliv.

71 Ibid.

72 Ibid., at xxxix.

to satisfy the requirements of the issuing statutes or applicable Attorney General Guidelines, and the final nineteen matters involved instances where the NSL recipient provided more information than that which was requested. Out of these 26 violations 15 violations occurred in investigations where an American was the target of the investigation, 8 violations involved investigations where the subject was a non-American individual, one violation involved a subject who was presumed to be a non-U.S. person, one violation involved a situation where there was no subject because there was no underlying investigation and in the final matter the status of the subject could not be determined.[73]

Out of the 22 possible IOB violations found by the OIG, one involved improper authorization, another 11 involved improper requests under pertinent NSL provisions, and the final ten involved unauthorized collections. According to these findings, there were errors in approximately 22 percent of investigations. Twelve of these errors were due to FBI errors while the other ten were errors made by the NSL recipient.[74]

An additional problem that the Inspector General noted in his report was the regular issuance of NSLs from control files, files that store information on individuals whom the FBI has not, and potentially may never, start an investigation on, rather than investigative files, which store the information on individuals whom are being actively investigated. This is a practice that is not permitted under FBI policy. The reason that this is so problematic is

> If NSLs are issued exclusively from control files the NSL approval documentation does not indicate whether NSLs are issued in the course of authorized investigations or whether the information sought in the NSLs is relevant to those investigations. This documentation is necessary to establish compliance with NSL provisions, the Attorney Generals NSI guidelines, and internal FBI policy.

73 Ibid.

74 Ibid., at xxxi – xxxii.

With the alarming number of problems that are able to be identified it is very troubling to consider the reality that there may be many additional errors existing from the NSLs improperly issued under these control files.

The most disturbing problem found by the Inspector General is the FBI's use of exigent National Security Letters. These exigent NSLs are the result of contracts that the FBI entered into with three different telephone companies in order to speed up the collection of telephone billing records and subscriber information.[75] In order to gain approval to obligate funds for these contracts the requests for approval for each of these contracts referred to the Counterterrorism Division's need to obtain toll billing information as fast as possible. These contracts obligated these phone companies to provide "near real time servicing" of legal process.[76]

Modeling these exigent NSLs after one used by the New York Division of the FBI to request phone records in connection with the FBI's criminal investigations of the September 11th hijackers, the Communication Analysis Unit issued over 700 exigent letters to the three phone companies between March 2003 and December 2005.[77] The FBI justified their actions by claiming "exigent circumstances" and that official National Security Letters were submitted to the Attorney General for process and service as soon as possible.[78] According to his audit the approximately 739 issued exigent letters requested approximately 3000 telephone numbers. This issue of exigent letters was again mentioned in the latest report issued by the Office of the Inspector General.

In his March 2008 report, the Inspector General argued that these exigent letters were signed by FBI Headquarters Counterterrorism Division personnel who were unauthorized to issue

75 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007. at xxxv.

76 Ibid.

77 Ibid.

78 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007. at xxxvi.

or sign them.[79] The Inspector General also noted that at times there were no pending national security investigations on the individuals targeted. The Inspector General stated that the problems with the FBI's filing system greatly diminished the amount of "reliable documentation to substantiate that NSLs or other legal process was issued to cover the records obtained" through exigent letters.[80]The Inspector General concluded this discussion by stating that an additional report was to be published solely regarding the FBI's use of these exigent letters. [81]

Based on these findings the Office of the Inspector General made ten recommendations to the FBI. These recommendations involved making corrections to nearly every step of their NSL procedure from original procedural corrections to storage collection corrections. These recommendations are discussed in detail in the second report where the Inspector General admits that the FBI has successfully made several of these corrections but, he concludes that problems still remain.[82]

1.7 Telecommunication Immunity Bill and its implications on National Security Letters

Recently, the role that telecommunication companies played in the aid of national security investigations was touched on by a new Congressional statute, *FISA Amendment Act of 2007*, s.2248. This statute as originally construed would have granted blanket immunity from suits by targeted persons to telecommunication companies who aided the intelligence community in conducting warrantless searches. This form of the bill, however, failed in the House of Representatives after gaining a clear majority in the Senate.[83] In response Representative John Conyers of Missouri sponsored *H.R. 3773 FISA Amendments Act of 2008*. This statute was

79 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters" edited by the United States Department of Justice, 2008 at 35.

80 Ibid.

81 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters" edited by the United States Department of Justice, 2007at xxxvi.

82 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters" edited by the United States Department of Justice, 2008.

83 S. 2248--110th Congress (2007): FISA Amendments Act of 2007, GovTrack.us (database of federal legislation) <http://www.govtrack.us/Congress/bill.xpd?bill=s110-2248> (accessed March 10, 2008).

renamed the Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act of 2007 or RESTORE Act of 2007. This act requires strict governmental surveillance of the actions of the intelligence community and a far more stringent approach to electronic surveillance.[84] In response to the heated debates over the passage of this telecommunication bill and the numerous errors found by the Inspector General, there has been a massive response by the media, various interest groups and several scholars.

This response has been both positive and negative. Some have argued that National Security Letters are better enabling the FBI to do protect citizens and are in perfect alignment with the federal statutes regarding the type of searches that they allow. Others have argued that these letters are unconstitutional and they result in widespread violations of several constitutional rights. Those in the latter category have argued that National Security Letter searches offend both their First and Fourth Amendment rights and for this reason they are unconstitutional and must be amended. While both sides of this debate make valid points I argue that National Security Letter searches violate an individual's constitutional rights. In my discussion, I focus solely on the Fourth Amendment and the challenges that I believe could and should be made on Fourth Amendment grounds. In the next chapter I provide a background on the Fourth Amendment and on precedents which are pertinent to National Security Letter Searches.

84 H.R. 3773--110th Congress (2007): FISA Amendments Act of 2008, GovTrack.us (database of federal legislation) <http://www.govtrack.us/Congress/bill.xpd?tab=main&bill=h110-3773> (accessed March 10, 2008).

Chapter Two: The Fourth Amendment

2.0 Introduction and Historical Background

The Fourth Amendment to the United States Constitution was adopted as a part of the Bill of Rights in 1789 and ratified by the states in 1791.[85] This amendment was designed to protect citizens from unreasonable searches and seizures and reads as follows:

> 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.[86]

The Fourth Amendment originated in direct response to the British practice of issuing general warrants and writs of assistance enabling them to enter one's home and search and seize items at their discretion. These general warrants were the subject of much contention within the colonies as evidenced by their presence in "*The Rights of the Colonists and a List of Infringements and Violations of Rights"* published in 1777 by Samuel Adams.[87] The problems that most Englishmen and colonists had with these general warrants were discussed in the English case *Entick v. Carrington* which involved Entick suing the government after they ransacked his home in search of documents belonging to or relating to John Wilkes.[88]

The colonies faced similar problems as a result of the use of "writs of assistance" a tool used by the British to enforce revenue laws. These writs of assistance were

> General warrants authorizing the bearer to enter any house or other place to search for and seize 'prohibited and uncustomed'' goods, and commanding all subjects to assist in these endeavors and once issued these writs remained in force throughout the lifetime of the sovereign and six months thereafter.[89]

---

85 Davis, Thomas. "Recovering the Original Fourth Amendment." Michigan Law Review no. December (1999). at 557.

86 The United States Constitution Amendment Four.

87 B. Schwartz, The Bill of Rights: A Documentary History (1971) 199, 205-06.

88 *Entick v. Carrington*19 Howell's State Trials 1029, 95 Eng. 807 (1705).

89 Find law U.S. Constitution: Fourth Amendment citing Quincy's Massachusetts Reports, 1761-1772, App. I, pp. 395-540, and in 2 Legal Papers of John Adams 106-47 (Wroth & Zobel eds., 1965). See also Dickerson, Writs of Assistance as a Cause of the

The ability for officers to use these warrants in such a broad manner agitated the colonists and led to unrest in the colonies.

2.2 Standards of Review

After facing tyrannical British rule and the constant fear of their privacy and homes being invaded by the use of British writs of assistance, the founders crafted the Fourth Amendment to protect citizens from these unannounced invasions into their privacy. While the exact meaning of the Fourth Amendment has been interpreted differently based on the context and the time period there have been certain standards established by the court to determine the validity of a Fourth Amendment challenge. One of the most pertinent standards established by the court for considering National Security Letter searches was the 1967 Supreme Court case *Katz v. United States*. In this case the Court was faced with the decision of whether the Fourth Amendment protected an individual's right to privacy when making a phone call in a public telephone booth. The Court held that an individual does have a right to privacy in the conversation that he has within a public telephone booth where he enters and shuts the door behind him. The Court held that even though the telephone booth is located in a public arena, the information within it was still considered private.

Whether someone has a privacy claim in their information is not determined by the location of the information, but in the context. For example, an individual does not have a Fourth Amendment claim to privacy in the actions he does in an open field, *Hester v. United States*, or in the information that he says in a crowded room. However, if even in the most public of arenas an individual acts in a way as to protect the privacy of what he is saying then he may have a right to privacy in that information that would justify a Fourth Amendment claim[90]. In the words of Justice Stewart:

American Revolution, in The Era of the American Revolution: Studies Inscribed to Evarts Boutell Greene 40 (R. Morris, ed., 1939).

90 *Hester v. United States* 265 U.S. 57 (1924).

> What a person knowingly exposes to the public, even in his own home or office is not a subject of Fourth Amendment protections but what he seeks to preserve as private, even in an area accessible to the public may be constitutionally protected.[91]

The court justified this argument by claiming that the Fourth Amendment "protect[s] people not places" and a Fourth Amendment claim is not determined by the "incantation of the term constitutionally protected area."[92] The Court ruled that the Fourth Amendment contains broad protections "the Fourth Amendment protects an individual's privacy against certain kinds of government intrusion, but its protections go further and often have nothing to do with privacy at all."[93] Based on this conclusion the court held that "the average man would very likely not have his feelings soothed any more by having his property seized openly than by having it seized privately and in stealth."[94]

Katz v. United States marked an important and notable transition for the Supreme Court from its former way of handling Fourth Amendment claims. In previous cases the court has interpreted the Fourth Amendment unreasonable physical searches and seizures of tangible items. The Court gradually moved away from this reasoning however, to an expanded interpretation of the Fourth Amendment. It was not until *Katz v. United States* that the court decided to set a new standard by officially overturning two previous decisions. These decisions were *Olmstead v. United States*, which held that the Fourth Amendment protects against only physical searches and seizures, and *Silverman v. United States,* which held that the Fourth Amendment protects only tangible items from being searched or seized.[95]

In making this change the court was cognizant of the implications that this broader interpretation of the Fourth Amendment could have. They knew that at least in so far as electronic searches and seizures were concerned there would have to be certain exceptions to typical Fourth

91 *Katz v. United States* 389 U.S. 347, (1967)at 351, 352.

92 Ibid., at 351.

93 Ibid.

94 Ibid., at 351.

95 *Olmstead v. United States* 277 U.S. 438 (1928) and *Silverman v. United States*, 365 U.S. 505 (1961).

Amendment procedure. For example, typically officers must announce their presence or inform an individual that they are conducting a search as a part of their compliance with a warrant, the Court understood that this advanced notice would nullify the effect of an electronic search. As a result the court held that "officers need not announce their purpose before conducting an otherwise authorized search if such an announcement would provoke the escape of the suspect or destruction of critical evidence."[96] They argued this knowing that "the very nature of electronic surveillance precludes its use pursuant to the suspect's consent."[97] The court held that while they are aware that "innocent citizens should not suffer the shock, fright, or embarrassment attendant upon an unannounced police intrusion" the problems that these announcements prevent, dangerous calling of police officers, are "not relevant to the problems presented by judicially authorized electronic surveillance."[98]

In discussing the particular case before them the court knew that the officers conducted a search without a warrant and conducted the search in such a minimally intrusive manner as would probably, reasonably have been approved by a judge. The Court, however, ruled that even though the officers acted with self restraint, the bounds of the search were determined by the agents themselves rather than a neutral judicial officer and this was problematic. For this reason:

> [The agents] were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notice the authorizing magistrate in detail of all that had been seized. In the absence of such safeguards this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end. Searches conducted without warrants have been held unlawful not withstanding facts unquestionably showing probable cause.[99]

96 *Katz v. United States* 389 U.S. 347 (1967) at 355.

97 Ibid.

98 Ibid., at 356.

99 Ibid., at 356 – 357.

In establishing this, the court focused on the importance of having a neutral magistrate to make the determinations on the specifics of a search in order to protect a citizen's rights. The court argues that "the constitution requires that the deliberate impartial judgment of a judicial officer be interposed between the citizen and the police."[100] This interplay is important for "the mandate of the (Fourth) Amendment requires adherence to judicial process." The court held that this interplay is required for a search to be reasonable, "searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions."

The Court understood the importance of recognizing that certain situations required different Fourth Amendment standards, but they held that in the absence of a judicial determination a search must still be reasonable. This applies to electronic surveillance investigations in the same way it would apply to any other type of investigation. This is even in cases where the agents claim they were acting in hot pursuit.[101] In fact, they argued that "there seems little likelihood that electronic surveillance would be a realistic possibility in a situation so fraught with urgency."[102] Justice Stewart concluded by saying that " wherever a man may be, he is entitled to know that he will remain free from unreasonable searches … bypassing a neutral predetermination of the scope of a search leaves individuals secure from the Fourth Amendment violations only in the discretion of the police."[103] As Stewart argues "omission of [a magistrate's] authorization bypasses the safeguards provided by an objective predetermination of probable cause, and substitutes instead the far less reliable procedure of an after-the-event justification for the search, too likely to be subtly influenced by the familiar shortcomings of hindsight judgment."[104]

100 Ibid., at 357.

101 *Katz v. United States* 389 U.S. 347(1967) at 358.

102 Ibid.

103 Ibid. 358 – 359.

104 Ibid.

While *Katz v. United States* left a strong precedent for understanding the Fourth Amendment, the importance of judicial authorization, and limitations on searches, the most important standard for determining how to judge the validity of a Fourth Amendment challenge came from Justice Harlan's concurring opinion. Justice Harlan argued that Fourth Amendment protections should be determined on the basis of whether an individual has a reasonable expectation of privacy in the information or place being searched or seized. To determine this he developed a reasonable expectation of privacy test based on the court's precedents. According to Justice Harlan:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and second, that the expectation be one that society is prepared to recognize as 'reasonable.'[105]

To apply his reasoning to the public phone booth at issue Justice Harlan argued that "the point is not that the booth is accessible to the public at other times…but that it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable."[106] From this argument, it is evident that Justice Harlan agreed that the Fourth Amendment is not limited by the arena in which one is and he recognized that privacy claims may exist even in arguably public locations. Justice Harlan also joined the court in their reasoning surrounding electronic surveillance. According to Justice Harlan, "reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[107]

While the Court stated in footnote 23 of the decision that issues of national security were not being addressed by this decision, Justice White used his concurrence to address this issue. In his determination, "we should not require the warrant procedure and the magistrate's judgment if

105 Ibid., at 361.

106 Ibid.

107 Ibid., at 362.

the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable."[108]

Justice Douglas and Justice Brennan disagree with this assessment and in their concurrence they argued that "neither the president nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be." They argued that accepting Justice White's view of executive authority would be as a "wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels 'national security matters.' Justices Douglas and Brennan agree that the privacy protections encapsulated in the Fourth Amendment apply to every citizen regardless of the type of crime they commit. For as Justice Douglas states:

> There is, so far as I understand constitutional history, no distinction under the Fourth Amendment between types of crimes. Article III s 3, gives 'treason' a very narrow definition and puts restrictions on its proof. But the Fourth Amendment draws no lines between various substantive offenses. The arrests on cases of hot pursuit and the arrests on visible or other evidence of probable cause cut across the board and are not peculiar to any crime. I would respect the present lines of distinction and not improvise because a particular crime seems particularly heinous. When the Framers took that step, as they did with treason, the worst crime of all, they made their purpose manifest.[109]

The arguments made by the Katz majority and the various concurring opinions all support raising the Fourth Amendment's protections of privacy and property to a level much higher than it had before. The Court argued that the goals of the Fourth Amendment demand that a system be put in place to ensure that searches are conducted in the least intrusive manner, a determination that they for the most part argue is only possible when a judicial magistrate is present. This is an important consideration in light of the use of administrative subpoenas, which the district courts have argued to be similar in some ways to National Security Letters, and the standards in place for Fourth Amendment claims when a third party is involved. I attempt to look at the standards set

108 *Katz v. United States* 389 U.S. 347 (1967) at 365.

109 Ibid., at 360.

for these contexts in order to use the next chapter to apply these standards to National Security Letters.

2.3 Administrative Subpoenas

In order to justify my overall argument that National Security Letters are unconstitutional I must first determine the standards under which they should be judged. In the cases mentioned in chapter one as well as in a majority of the current scholarship, National Security Letters have been likened to administrative subpoenas. While administrative subpoenas do share a few similarities, I argue in chapter three that they are substantially different from National Security Letters. I use this section to introduce administrative subpoenas, to explain the relevant precedents, and to determine the standard under which the validity of an administrative subpoena is challenged.

An administrative subpoena is a tool that nearly 350 different federal agencies posses to assist in their investigations. [110] Administrative subpoenas have far less exacting standards than warrants to justify their use. There are two different types of administrative subpoenas, "the subpoena ad testificandum, which orders a witness to appear and give testimony, and the subpoena duces tecum which requires the production of documents or a showing of cause why they need not be produced."[111] Administrative bodies may only gain subpoena power through a legislative statute.[112] The Supreme Court has held, however, that once an agency obtains the power to issue administrative subpoenas, the agency head may delegate this power, a strategy the authority of which may be inferred from the agency's duty to promulgate rules and regulations.[113]

To challenge the reasonableness of an administrative subpoena there are three important factors that must be taken into consideration: jurisdiction, reasonableness and constitutionality. *Oklahoma Press Publishing Co. v. Walling* is an important precedent regarding the jurisdiction of

110 Ibid., at 6

111 McKnight, Deborah K., Administrative Subpoenas Information Brief for the Minnesota House of Representatives Research Department at 2 http://www.house.leg.state.mn.us/hrd/pubs/adminsup.pdf Date Accessed: March 1, 2008.

112 Ibid.

113 *Fleming v. Mohawk Wrecking and Lumber Co*. 331 U.S. 111 (1947).

an agency to issue administrative subpoenas. In Walling, the Supreme Court held that the scope of an agency's statutory authority cannot be litigated in judicial proceedings to enforce an administrative subpoena.[114] Rather than challenge the jurisdiction in which an administration may issue a subpoena most challenges to administrative subpoenas are based on reasonableness grounds. Administrative subpoenas, as distinguished from warrants have a far more minimal reasonableness standard. To determine the reasonableness of a subpoena, the Supreme Court in *Oklahoma Press* established a three prong test: the investigation must be legitimate, the subpoena must not be overly broad, and the information sought must be relevant to the investigation.[115]

Administrative subpoenas are typically challenged in court on Fourth and Fifth Amendment grounds. In *Marshall v. Barlow's* Inc and *Donovan v. Dewey* the Supreme Court articulated its position on the constitutionality of administrative subpoenas under the Fourth Amendments reasonableness standard. In *Marshall v. Barlow's Inc,* the Supreme Court held that the Fourth Amendment's protections against unreasonable searches and seizures apply to requests for information, and in *Donovan v. Dewey*, the Court held that while certain warrantless administrative searches are acceptable, in some circumstances the Fourth Amendment may require a warrant to ensure that the search and seizure is not unreasonable.[116] Many challenges are made under the Fifth Amendment's protection against self incrimination. In *Couch v. United States* the Supreme Court held that this privilege may only be asserted by an individual, and may not be made by a corporation or a union.[117]

While administrative subpoenas justify broad searches by certain statutorily empowered agencies these searches are not without their limitations. One of the most relevant limitations on

114 *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946).

115Ibid.

116 *Marshall v. Barlow's Inc*., 436 U.S. 307, (1978) and Donovan v. Dewey 452 U.S. 594 (1981).

117 *Couch v. United States* 409 U.S. 322 (1973).

administrative subpoena authority is that they may not be used in terrorist investigations.[118] This limitation is coupled with the fact that administrations with subpoena authority may only issue administrative subpoenas to gather information relevant to that particular agency. For example, the IRS may subpoena an individual's financial records, but, it would be arguably an abuse of their authority for them to request an individual's phone and email records.

While scholars like Daniel Bohl, mentioned in the above literature review, have argued that National Security Letters should be held only to the minimal standards used by the Courts in determining the validity of an administrative subpoena claim, others question who really should have standing to challenge these claims even under these minimal standards. In arguing for why individuals should not have the right to challenge a national security letter search of their information the government draws on two Supreme Court precedents which deal with searches and seizures of the information stored by a third party.

2.4 Third Party Intervention

There are two important precedents regarding the effect that a third party has on an individual's Fourth Amendment claims. While these cases were only regarding narrow questions the precedents established in them have been broadly applied. In fact, these cases have established a Fourth Amendment standard for determining the reasonableness of searches into the records of any third party.

According to the Supreme Court, if an individual chooses to discuss information with a third party he lacks a reasonable expectation of privacy in that information. In both *Smith v. Maryland* and *United States v. Miller*, the Court justified collection of information under the minimal procedural safeguards contained in an administrative subpoena.

In *Smith v. Maryland*, the Supreme Court dealt with the issue of whether an individual has a reasonable expectation of privacy in the numbers dialed on a phone. In this case the Supreme

118 Doyle, Charles: Administrative Subpoenas and National Security Letters in Criminal and Foreign Intelligence Investigations: Background and Proposed Adjustments Congressional Research Service The Library of Congress. 1 FN. 1.

Court ruled that the fact that modern technology replaced the existence of an old fashioned phone operator with an automated service, a set up under which they agreed that the complainant would not have a reasonable expectation of privacy, does not make once accessible information inaccessible to investigators.[119] In chapter three I contest this assertion that an individual would not have a reasonable expectation of privacy in the phone numbers dialed.

In *United States v. Miller* the Supreme Court was asked to determine whether an individual has a right to privacy in their financial information held by a bank or financial institution. In *Miller* the Court held that an individual does not possess a right to privacy in these records because they are exposed to its various employees. The Court further extended the impact of this ruling by claiming that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.[120]

In the following chapter I look at these various precedents and standards and apply them to National Security Letters. I attempt to distinguish NSL searches from those implicated in the aforementioned precedents and I argue that they deserve a far more stringent judicial standard.

119 *Smith v. Maryland* 442 U.S. 735 (1979).

120 *United States v. Miller* 425 U.S. 435 at 441 – 443.

Chapter Three: Applying the Fourth Amendment to National Security Letters

3.0 Introduction

In this chapter, I apply the Fourth Amendment standards discussed in the previous chapter to National Security Letter searches. I begin by discussing the information that these letters give the government access to and considering whether there is a reasonable expectation of privacy in this information. I then apply the precedents established regarding information given to a third party and those regarding administrative subpoenas to National Security Letter investigations. I argue that there is a reasonable expectation of privacy in electronic information and for this reason National Security Letter searches must be viewed in light of a balancing test.

The ability of the government to seize and scrutinize the information surrounding an individual's internet usage, financial information, phone records, and electronic communications without any prior judicial review is arguably at odds with the Fourth Amendment. This is especially true if looked at from a historical context with knowledge that this amendment was construed for the purpose of avoiding governmental use of "writs of assistance" or general warrants. These writs of assistance did not require individualized suspicion of their target. This gave them access to an individual's person and property with limited procedural safeguards. While National Security Letters do require individualized suspicion, in some cases, this is not the case when a suspect's contacts are targeted. In light of this similarity it seems highly implausible that National Security Letters would be considered acceptable under the original intention of the founders.

3.1 Electronic and Financial Information

We are living in an age of technology. In today's world a great deal of information about an individual is recorded in databanks and computer systems, from medical records to consumer purchases. Modern technology has enabled a majority of corporations to create electronic files detailing consumer information. Digital information has enabled companies to save thousands of dollars as it is both cheaper than paper forms, which must be stored, and far easier to organize and

access. The invention and use of the internet provides a new medium vastly affecting the privacy of this digital and electronic information. The internet contains massive amounts of multifaceted data on individuals. Today, it is possible to use the internet to conduct banking, make travel arrangements, shop, research items of interest, make phone calls, interact with individuals across the globe and much more. This digitalization of information is particularly poignant in a world where it is nearly impossible to live without relying in some way on third parties. For this reason I argue that the existing precedents on third party searches should not be the sole guiding light in judging the use of national security letters. To justify this claim, I attempt to distinguish National Security Letter searches from Third Party information requests.

3.2 The Reasonable Expectation of Privacy in this information

Modern technology creates an ease of access to both private and public information. This ease of access does not justify broad searches by the government and should require the strict scrutiny of investigations because of the potential for abuse. This requirement is especially necessary when investigations target the vast information on individuals held by financial institutions, phone companies, electronic communication providers, and internet service providers. *Katz v. United States*, as discussed above, is arguably one of the most pertinent precedents for studying the constitutionality of National Security Letters. In order to apply this precedent to National Security Letters it is important to determine whether there is a reasonable expectation of privacy in the information that the FBI is able to obtain through National Security Letter searches.

3.21 Justice Harlan's REOP test applied

In applying the Katz precedent to National Security Letters Justice Harlan's REOP test can be applied to National Security Letter Searches.

3.21(a) Subjective Expectation of Privacy

Individuals show a subjective expectation of privacy in their electronic, phone, and financial information in several ways. Individuals typically must use a personalized identification number

(pin) in order to gain access to their financial records from Automatic Teller Machines (ATM) or to make purchases with a debit card. Often financial companies also require the use of a personal password and username combination along with pin number and knowledge of a particular account number prior to giving an individual access to information on the specifics of an account. This is especially the case with banks and many federal loan websites, such as Free Application for Federal Student Aid (FASFA). Other financial institutions offer different forms of these types of privacy protections to ensure that the information on their customers does not get improperly released.

Financial institutions are not the only institutions whose websites and account information systems require levels of privacy protection. Electronic information stored online is often protected by a password and username combination. In fact, many websites, particularly those that contain private information or are related to financial transactions, have password and username strength tests to determine the security of that combination choice. Many internet service providers use passwords and usernames to allow customer's access to the internet to ensure that only authorized individuals may use their service. Arguably, entering a private password protected area online could be likened to shutting a public pay phone door behind you. In addition, just like a pay phone is in a public arena some argue the internet should be considered a public arena. For this reason, the Supreme Courts holding that one has a reasonable expectation of privacy in the payphone, despite the fact that it is located in a public arena, can be used to argue that an individual should also hold a reasonable expectation of privacy in electronic information.[121]

Some individuals go even further to protect their privacy and create an encryption code or use encryption software to encrypt the information they communicate online in order to ensure its

121 *Katz v. United States* 389 U.S. 347 (1967) at 511.

privacy.[122] In addition, individuals sometimes express an expectation of privacy in electronic information by stating personal claims on a private blogging site and by conducting searches on personal information or circumstances. Certain individuals take additional privacy measures in their phone conversations as well by choosing to make their phone numbers "private" or "restricted" so that the person whom they call does not know their phone number, information that would not be accessible without the aid of the service provider. It would seem that this would be a fruitless practice if they believed their privacy could be invaded through a National Security Letter information request.

3.21(b) Society's Objective Expectation of Privacy

I argue that society regards as objectively reasonable an expectation of privacy in the information that may be collected during a National Security Letter search. One of the first examples of society's view that this information deserves extra privacy protection is the original Congressional intent for enacting the four statutes that contain national security letter provisions. Most of these statutes were enacted by Congress to add extra layers of privacy protection to, ironically, precisely the information that an NSL authorizes the FBI to obtain. Congress originally justified the existence of these NSL provisions by claiming that they were only to be minor exceptions to aid in FBI foreign intelligence investigations, as mentioned above. While it is true that Congress also agreed to the passage of the United States Patriot Act, I argue in the next chapter why this approval should be considered differently.

Second, society shows an objective expectation of privacy in their acceptance of the numerous services dedicated to the protection and security of digital, electronic, and other private information. These services which include software security analysts and cryptographers have not only been welcomed into the market but they are often in high demand. Currently, there are

122 Encryption is defined as "the coding of a clear text message by a transmitting unit so as to prevent unauthorized eavesdropping along the transmission line; the receiving unit uses the same algorithm as the transmitting unit to decode the incoming message," "encryption." McGraw-Hill Dictionary of Scientific and Technical Terms. McGraw-Hill Companies, Inc., 2003. Answers.com 03 Apr. 2008. http://www.answers.com/topic/encryption.

numerous companies and corporations dedicated to the protection of privacy and preventing information from being accessed by prying eyes. Often the corporations and individuals who use this service could arguably be seen as showing that they feel this information should receive extra privacy protection because it is personal and because currently this area is not as protected as it could and should be.

Finally, many internet service providers, phone companies, and electronic communication service providers have privacy policies detailing their role in protecting a client's privacy in their information. For example, AOL's Internet Privacy Policy contains the following statement:

> The contents of your online communications, as well as other information about you as an AOL Network user, may be accessed and disclosed in response to legal process (for example, a court order, search warrant or subpoena); in other circumstances in which AOL believes the AOL Network is being used in the commission of a crime; when we have a good faith belief that there is an emergency that poses a threat to the safety of you or another person; or when necessary either to protect the rights or property of AOL, the AOL Network or its affiliated providers, or for us to render the service you have requested.[123]

Most internet service providers have similar clauses stipulating their compliance with any judicial inquests into their records. Several ISPs even offer certain privacy options to their customers who feel their information warrants extra protection. Certain companies like Road Runner and AOL enable their clients to decide whether their information will be disseminated to private consumer marketing firms and if so to what extent.

These actions on the part of legislatures, private actors, and individual consumers prove that there does exist at least in some circumstances an expectation of privacy within the information accessible to the FBI under their NSL search authority. This expectation of privacy justifies the need for additional procedural safeguards to be put in place to protect the sanctity of this information.

123 AOL privacy policy found at http://about.aol.com/aolnetwork/aol_pp accessed March 3, 2008.

Based on this claim the information that National Security Letters authorize the FBI to request is information in which an individual has a reasonable expectation of privacy. I now look at a hypothetical scenario where National Security Letters were issued and how they can and should be challenged as unreasonable searches under the Fourth Amendment.

3.3 The Case of Jane Smith and Johnny Doe

The FBI has the sole determining authority in deciding how to handle National Security Letter Investigations. They decide who to investigate, when, and to what extent. In order to explain how National Security Letter searches can effect an individual I will discuss the hypothetical cases of Jane Smith and Johnny Doe. Jane Smith is an American citizen attending a public university in Florida. Jane is an independent student and she is working her way through school and paying her taxes each year. Jane has multiple email accounts in her name from various service providers each with their own unique password and username combination. Jane also has a cellular phone and has purchased a contracted plan from a service provider. Jane has a student credit card which she uses to do online shopping and pay for her schooling. Jane also has access to the internet which she pays for monthly. Jane uses this service to conduct school related and personal research and to meet and chat with people who share similar interests. Jane is also a member of an online chat community and she pays a nominal monthly fee for this service.

Currently, Jane is continuing her life as she normally would while unbeknownst to her the FBI is pouring over her records which they obtained through their ECPA, RFPA, and FCRAv national security letter authority. While studying her records the FBI discovered that their search into her background was unsubstantiated insofar as any terrorism or clandestine intelligence activity. However, they felt that Jane could lead them to other suspects so they decide to investigate all 100 individuals on Jane's e-mail and phone contact lists that they obtained under the ECPA NSL. One of these contacts was Johnny Doe.

Johnny Doe was an American citizen living in Washington D.C. Johnny is a member of the same chat community as Jane and he paid his monthly fees. Johnny and Jane met in one of the

chat rooms in this community. Over the past several years Jane and Johnny have emailed each other a few times very sporadically. Jane and Johnny have never met and have never spoken on the phone. Yet, now the FBI is using their full NSL authority to gather records on Johnny.

While the FBI was unable to find anything in Johnny's records to corroborate a suspicion of terrorism or clandestine intelligence activities, they believed that there still may be more information that they could get through other investigative techniques and they wanted to stall Johnny from doing acts they feared he might be capable of. In order to stall Johnny the FBI studied his financial records and credit report carefully and noticed that some of the activity seemed questionable. The FBI decided that there was enough evidence for a potentially criminally actionable fraud charge. In order to corroborate this belief they discussed their findings with a prosecutor at the United States District Attorney's Office, who, as mentioned before, has equal access to this information.

The prosecutor agreed that the records seemed to suggest fraud and she decided to officially begin a fraud investigation on Johnny Doe. The prosecutor may not use this information in trial without offending the criminal discovery process.[124] The prosecutor also may not use this information without offending the FBI's investigation because enabling the prosecutor to use this information would give the defense and others access to these records. However, the prosecutor has the definite advantage of knowing where to look for the information and has a pretty good idea of what an investigation will reveal. Pursuant to these proceedings Johnny Doe is arrested on charges of fraud and is found guilty in a court of law. Several other individuals on Jane's contact lists were investigated as well. While most of those investigations proved fruitless the FBI was able to turn over information to the IRS on a few individuals whom they noted as having

124 Typically a prosecutor must follow Fourth Amendment procedure in collecting information and may use subpoenas and warrants to obtain information. This information is then accessible by both parties in order to prepare for trial. Because of the secrecy surrounding National Security Letter Investigations, a defense attorney would not be allowed access to this information and more than likely it would not be information that could be used in a open court proceeding. For this reason the attorney must use other legally acceptable means to collect the same information that the FBI made him aware of.

questionable financial records yet they did not believe they could substantiate a fraud claim. Based on this information the IRS decided to audit several of these individuals, and the FBI is pursuing further administrative action.[125]

There are thousands of colleges across the nation filled with students who live their lives in nearly the same manner and potentially millions of individuals who share at least one or two circumstances, such as having an email account or a cellular phone. This is particularly true as the internet continues to expand as a media for communication and research. What distinguishes Jane from any other individual with an email, phone, or credit account, or even from someone who has conducted any recorded financial transaction? Why Jane? Why Johnny? Who decides and who should? Why should we continue to give the FBI the sole discretionary authority to conduct these National Security Letter Searches especially after reading the numerous errors and power abuses that the Inspector General noted in his report?

Another important concern is the vast number of individuals who may access this information. In "FBI Unbound: How National Security Letters Violate Our Privacy," a documentary by the Bill of Rights Defense Committee, viewers are informed that any information obtained by the FBI through NSLs will be prepared into files and stored in an Information Data Warehouse to which over 12,000 private and government actors will have access.[126] This dissemination of information beyond the FBI was partially a result of Presidential Executive Order 13388 which calls for:

> The interchange of terrorism information among agencies; (iii) the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal governments, and between agencies and appropriate private sector entities; and (iv) the protection of the ability of agencies to acquire additional such information.[127]

125 Office of the Inspector General. "A Review of the Federal Bureau of Investigations Use of National Security Letters ", edited by United States Department of Justice, 2007.

126 Bill of Rights Defense Committee "FBI Unbound: How National Security Letters Violate Our Privacy" [documentary].

127 Presidential Executive Order 13388.

President George W. Bush's explicit intent behind this statute was to "maximize the utility of the information in protecting the territory, people, and interests of the United States."[128] To comply with this presidential mandate the FBI and other groups created the Information Data Warehouse (IDW) in January of 2004 to store the information received by the various departments.[129] In 2003, one year prior to the creation of the IDW, Attorney General John Ashcroft changed the existing FBI procedure by:

> rescind[ing] a 1995 guideline directing that information obtained through a national security letter about a U.S. citizen or resident "shall be destroyed by the FBI and not further disseminated" if it proves "not relevant to the purposes for which it was collected." Ashcroft's new order was that "the FBI shall retain" all records it collects and "may disseminate" them freely among federal agencies. The same order directed the FBI to develop "data mining" technology to probe for hidden links among the people in its growing cache of electronic files.[130]

This important change to department policy has had a lasting impact. This stored information now allows the FBI to have access to this information at a later date without having to conduct another search.[131] In fact, one aspect of the IDW is that it contains information gathered from other search techniques used by other agencies. This type of database gives the FBI access to information that they would have either been unaware of or statutorily prohibited from requesting for themselves. In fact, this database enables every individual who has access to it to obtain information that they potentially never would have or could have. The government, in its diverse roles, has authority over individuals and could use this information to begin criminal and administrative proceedings. The ability of the government to use this information in ways that could hinder or harm an individual has terrifying implications for the future of privacy rights in information and is another reason why we should not continue to defer to the FBI in determinations regarding national security letter searches.

---

128 Ibid.

129 Barton, Gellman. ""The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans." The Washington Post, November 6, 2005. at AO1.

130 Ibid.

131 Ibid.

Government intrusion into the private lives of American citizens is far different than private intrusions into privacy. There is always the potential that private information could fall into the hands of another private individual who desires to use this information to harm the individual whom they have the information on. However, the likeliness of an individual's ability to gain accidental or improper access to the same amount of information that the FBI may obtain under its NSL authority is very unlikely for several reasons. First, private individuals do not have the authority to search and demand information, and second, while private individuals can threaten to take their information to the government, they will still only have certain things they can do with it. A private individual does not have the authority to continuously obtain private data to take to a prosecutor in attempt to establish a criminal liability. A private individual is also not capable of limiting an individual's liberties to the same extent that the government is capable of.

For these reasons there should be procedural safeguards put in place to restrain the government's authority and to act as an intermediary between the investigator and the suspects. This argument is supported by the Supreme Courts holding in *Katz v. United States* that "the Constitution requires 'that the deliberate, impartial judgment of a judicial officer be interposed between the citizen and the police."[132] In the case of National Security Letters there is no impartial judicial officer between the citizen and the police. The FBI has a direct connection to information on a citizen without the citizen ever being aware. The sole barrier between the FBI and the information is a third party institution with arguably very limited incentive to challenge a National Security Letter request. Realistically, there is a tremendous cost both monetary and in regards to the time that must be expended by these third parties simply in order to fulfill a National Security Letter's request for information, particularly when the information requested is on multiple people. This cost may potentially limit the incentive for a company to take on the further costs of challenging a request if they are uncertain whether they will win. Also any

132 *Katz v. United States* 389 U.S. 347 (1967) at 514 citing: *Wong Sun v. United States* 371 U.S. 471, 481-482 at 441.

additional costs from arbitration may be prohibitive if a company is unsure if it will be able to fulfill the request if it loses in court.

The recent Telecommunication Bill debate that is occurring in Congress and the executive branch adds an interesting perspective from which to view incentives and disincentives for challenging NSLs. This debate comes down to whether telecommunications companies who contracted with the FBI and provided them information in warrantless searches should be immune from civil liability for their actions. In order to fully discuss the incentive structure I look at both sides of the debate in attempt to prove why I believe that the companies should receive immunity, with one exception.

If these telecommunications companies are not granted immunity for their actions they still would have limited incentive to challenge their receipt of National Security Letters in court, for the reasons mentioned above. Typically, National Security Letters have a stringent non-disclosure provision attached to them. This non-disclosure provision would prevent the consumers from ever finding out that the company received an NSL request and that their records may have been searched. Telecommunication companies would then be faced with the decision of whether they should challenge this request. If they challenge the letter they risk facing the costs of the litigation as well as the potential that their receipt of an NSL would be made known to a number of additional individuals and could potentially become public knowledge, depending on what grounds they challenged the claim.

The mere fact that the FBI can assert that NSL searches are within their authority, and the fact that they can show a statutory basis for this power, often works as a disincentive for corporations and has the effect of making it seem as if their attempts to challenge this search would be fruitless.[133] This claim is supported by the fact that since the addition of explicit judicial review by the Reauthorization Act the number of NSLs issued continues to rise while the public

133 This argument is based off of the argument posed by Judge Marrero in *Doe v. Ashcroft*, when he argues that the ominous wording of the statute could have prohibited some recipients from believing they may challenge a NSL.

has not been made aware of any new challenges made against NSLs. I argue that while granting immunity would limit the incentive to challenge NSLs even further, the third parties involved should only be liable if they filled requests in the manner that is not statutorily authorized, such as providing information beyond what the request is for or providing the information prior to receipt of a NSL. If, however, they followed the law, or what they in good faith believed the law to be, they should not be held legally liable.

3.3 Information given to a Third Party Precedents distinguished from NSL searches

Nearly all of the privacy agreements of the major internet service providers contain a clause stating their willingness to cooperate with local and federal law enforcements and supply the information that they request. This seems to be a reasonable provision in order for a telecommunication provider to lawfully exist within any society ruled by laws. In essence, these telecommunication providers are relying on the law to ensure privacy and to ensure that the constitutional guarantees are assured. It would be unreasonable to expect telecommunication providers to refuse compliance with legal officials and enforcement agencies. Instead, we must ensure that the laws under which they are governed are reasonable and provide protection from both illegal activity as well as invasive governmental intrusion on our private lives. When the government fails to do this it should be liable and be able to be challenged.

3.4 Challenging a National Security Letter:

The government has tried to justify its continued use of NSLs on the grounds that after the fact judicial review has now been made explicitly available to all NSL recipients. However, the existence of judicial review begs the question of who really has the authority to challenge these letters and on what grounds. It appears without question that an NSL recipient should have the right to challenge the non-disclosure provision of NSLs on First Amendment freedom of speech grounds. Yet, do they really have Fourth Amendment grounds to challenge these NSLs? Yes, I believe they do, however, only in a very limited sense. Internet Service Providers do have the information that is stored in their computers searched and while not being forcibly seized they

are being formally requested with threat of judicial liability for non compliance. Yet the information that National Security Letters request is not information on the recipient it is information regarding their clients. I argue that these letters should be able to be challenged by those individuals whose information is obtained through National Security Letter Searches. However, the questions arise as to whether the individual whose records have been obtained has Fourth Amendment grounds to challenge these letters and if so what standards should be used by the courts in deciding whether a reasonable search was conducted.

3.5 Distinguishing third party searches from National Security Letter Searches

To determine whether an individual should be able to challenge an NSL investigation on Fourth Amendment grounds it is important to return to the precedents on third party searches. As discussed in the previous chapter any information in the hands of a third party has been held to deserve less protection as a result of the Supreme Court's decisions in *United States v. Miller* and *Smith v. Maryland*. National Security Letter searches can be distinguished from the searches at issue in these cases. In addition, these precedents are overly broad and National Security Letter searches have proven this overbreadth. I also disagree with the court that there is not a reasonable expectation of privacy in this information for two reasons. First, just because modern technology has created an ease of access to this information does not mean that we have authorized its collection and distribution to the government and beyond. Second, there is far more personal information that can be uncovered from these searches that the court does not address.

As discussed above, the Supreme Court held in *Smith v. Maryland* that an individual does not have Fourth Amendment privacy grounds to challenge the use of a pen register which captures data on all of the phone numbers dialed by a particular phone line. They ruled that an individual does not have a legitimate expectation of privacy over this information because they conveyed the numbers over the phone lines which were recorded by the phone company. They held that even if a phone number is dialed within a home a person has no reasonable expectation of privacy in that number because they have revealed it to a third party.

Pen registers only record the numbers dialed on a phone line while it is attached, it does not collect a complete contact list on individuals nor can it record the numbers that have called in or been dialed before it was attached or after it was removed this is in contrast to the information that NSLs authorize the FBI to obtain. While an individual is more than likely aware that a phone company records this information in order to conduct legitimate business, such as billing customers for long distance calls they make, and the phone company in the same way records all of the numbers that have dialed a phone number, an individual never consented for these records to be turned over to the FBI and then disseminated.

While the court held that the telecommunication company's decision to share this information is an implicit risk in using a phone service, we must look at the breadth of information that can be revealed. First, an individual's phone activity can reveal many things such as who the person chooses to communicate and associate with, the identification of several members of the suspect's family and close friends as well as any businesses that an individual decides to contact. Mere knowledge of the fact that our phone activity can be, and is, recorded for legitimate business reasons does not equate our consent for all of this information to be revealed to the FBI who is looking for this exact information in many cases. Modern technology has enabled the phone company to record more information than it was capable of obtaining when operators were used to connect individuals. For these reasons, I think that the holding in *Smith v. Maryland* should be distinguished from National Security Letter search investigations.

According to the court, we may not have a reasonable expectation in the numbers that we dial however, we do have a reasonable expectation of privacy in whom we choose to associate with and the friends, family members, businesses, and acquaintances we have and choose to contact. FBI agents are not capturing this information simply to look at the numbers and match up the numbers dialed. Instead they analyze this information and obtain from it what they can. For this reason, an individual should have a reasonable expectation of privacy in these phone numbers. Just because modern technology enables the FBI to obtain this information and because

we must rely on a third company to provide us the phone services that our society relies on to stay connected does not justify the government's ability to seize, analyze, and disseminate these records. This is especially the case when the FBI is obtaining these numbers without individualized suspicion, a factor that existed in the case of *Smith v. Maryland*. In addition, the FBI should be limited from obtaining the records of potentially thousands of individuals with one NSL.

In *Smith v. Maryland*, the Supreme Court relied in part on its holding in *United States v. Miller*. In *United States v. Miller*, as discussed in chapter two, the Supreme Court held that an individual does not have a right to privacy in information he openly shared with the bank. The Court held that the fact that the bank uses this information in their legitimate business activities is another reason to limit the privacy claims that an individual has over this information. While a third party may access the information for their own record keeping this does not give them the authority to give it out to the government. There is of course certain financial information that individuals must give to the government each year. This information includes, but is not limited to, tax information, financial records needed for federal financial aid, and financial information required for federal welfare programs. National Security Letter investigations request a much greater amount of information than the government requires citizens to produce. We need not send the government a detailed list of all of our financial transactions, web searches, web sites visited, phone numbers dialed and received, and credit report history, a third party should not be able to take it without our permission and without our even knowing. The mere fact that a third party is involved does not mean that we authorize them to share our information. It must be noted that I am distinguishing the instances where individuals do explicitly consent through user agreements from the many instances where these agreements are never made nor signed.

Financial information has an even greater potential then phone activity data to reveal personal information about an individual. From a record of what an individual spends their money on people can learn personal taste in clothes, food, music, books, etc, as well as the groups

and organizations to which an individual may donate to including religious, political, and entertainment groups. Financial information can also reveal sources of income and any financial investments such as stocks and bonds. Financial transactions can reveal certain vices such as the amount of alcohol one purchases and gambling transactions. Financial transactions can even reveal highly sensitive information such as the medical procedures purchased with a credit card and the drugs purchased from a pharmacy or drugstore. Financial information that is used by a bank or a financial institution for their recordkeeping, or the type that must be disseminated to the government is far different from what the FBI is looking for in an individual's financial transaction information, credit history, and account records. The FBI is searching for the personal information that can be derived from these records. In this way the searches that National Security Letter provisions authorize can be distinguished from *United States v. Miller*'s holding.

The searches involved in both *United States v. Miller* and *Smith v. Maryland* can be distinguished from National Security Letter searches. The broad information that can be obtained from these searches expands as technology continues to advance. I argue that individuals should be able to challenge National Security Letter searches on Fourth Amendment privacy grounds especially with the fact that National Security Letters may be used to search electronic information, information which was not discussed in either *U.S. v. Miller* or *Smith v. Maryland*.

Following this argument it is important to discuss what standards should be used by the court in their determinations on the validity of National Security Letter searches. For this reason I now compare NSLs to administrative subpoenas, mentioned in chapter two, and I argue that they can and should be distinguished. For this reason, National Security Letter investigations should meet stronger procedural standards than the minimal standards required for administrative subpoenas.

Administrative subpoenas are quite different then National Security Letters in many ways. First, the processes surrounding administrative subpoenas is very open allowing numerous

opportunities for a party opposing the request to challenge the materials in the courts.[134] This openness is in stark contrast to National Security Letter searches which are cloaked in secrecy and imply standing only for the NSL recipient, not for the individual whose records are to be searched. Second, the FBI's broad investigation jurisdiction typically makes NSL searches far broader then administrative subpoenas as they can only be used if there is a legitimate purpose and the inquiry is related to that purpose and most agencies and administrations with this authority have limited types of information with which they are concerned and their limited purpose for requesting it. For example, the IRS is only interested in financial records to ensure that taxes have been appropriately paid. Third, administrative subpoenas may not be used in terrorism cases whereas National Security Letters are designed specifically for that purpose. This is especially important to consider in light of the effect of terrorism on the American mindset and the political and social climate that the country has been in since September 11th, 2001.[135] For these reasons National Security Letters can and should be distinguished from administrative subpoenas and should be held to a different, and stronger, standard of judicial accountability.

As I have argued National Security Letter searches can be distinguished from the third party searches at issue in *United States v. Miller* and *Smith v. Maryland* as well as from administrative subpoenas. For these reasons individuals should be able to challenge a national security letter search of their records. Because this type of challenge has not as yet occurred I propose the consideration of a hypothetical challenge to national security searches on Fourth Amendment privacy grounds conducted by an individual whose records have been searched. In

134 Weiner, Lauren M. "Special" delivery: where do National Security Letters fit into the Fourth Amendment? Fordham Urban Law Journal 33.5 (Nov 2006): p1453 (29).

135 During President George H.W. Bush's speech on Homeland Security at the FBI Academy in Quantico Virginia on September 10, 2003 President Bush made the following statement: "Administrative subpoenas, which enable law enforcement officials to obtain certain records quickly, are critical to many investigations. They're used in a wide range of criminal and civil matters, including health care fraud and child abuse cases. Yet, incredibly enough, in terrorism cases, where speed is often of the essence, officials lack the authority to use administrative subpoenas. If we can use these subpoenas to catch crooked doctors, the Congress should allow law enforcement officials to use them in catching terrorists."

responding to this challenge I argue that the courts should view National Security Letters in light of a balancing test. For as Fred H. Cate argues

> One individual's privacy interests may conflict with another's, with the interests of society, or even with others of his own interests. What is needed is a balance, of which privacy is a part. Determining what that part is in any specific context requires a careful evaluation of subjective variable and competing interests.[136]

In the next chapter I balance National Security Letters on this type of scale.

136 Cate, Fred H. Privacy in the Information Age Brookings institution Press Washington, D.C. 1997 Washington D.C. at 31.

Ch. 4 Balancing Act

4.0 Introduction

Having examined what National Security Letters are, what the Fourth Amendment protects, and how the precedents should be applied, I now return to the hypothetical I discussed above where an individual challenges the constitutionality of the FBI's current use of National Security Letters. I begin by looking at both national security and the value of privacy. Then I weigh the national security that these letters afford and the value of the privacy in the information they provide on a balancing scale. Current National Security Letter provisions fail this balance to the detriment of privacy rights.

While both of these values are vital and imperative to a society they often clash and at that point it is important to determine if a balance is reached, and if not, how to correct the imbalance. This is particularly important with National Security Letters, which have the potential of changing the course of criminal, intelligence, and national security investigations. For as Lauren Weiner argues, "[t]he potential for abuse of NSLs is certainly great, but the answer to the question of 'reasonableness balancing' may turn on one's view of which is more important: civil liberties or national security."[137]

The fact that our nation is currently in a time of war, and national uncertainty makes it imperative that this balance not be taken lightly

Striking the proper constitutional balance here is of great importance to the Nation during this period of ongoing combat," wrote Justice Sandra Day O'Connor in the Hamdi decision. "But it is equally vital that our calculus not give short shrift to the values that this country holds dear or to the privilege that is American citizenship. It is during our most challenging and uncertain moments that our Nation's commitment to due process is most severely tested; and it is in those times that we must preserve our commitment at home to the principles for which we fight abroad.

137 Weiner, Lauren M. "Special" delivery: where do National Security Letters fit into the Fourth Amendment? Fordham Urban Law Journal 33.5 (Nov 2006): p1453.

[A] state of war is not a blank check for the President when it comes to the rights of the Nation's citizens.[138]

4.1 National Security

National Security is one the nation's most important and time honored responsibilities. As noted by Judge Marrero, "National security is a paramount value, unquestionably one of the highest purposes for which any sovereign government is ordained."[139] While protecting a nation and its citizens is a vital responsibility, the term "national security" has been defined in many ways. The Executive Branch currently defines National Security broadly, claiming that "National Security includes the defense of the United States of America, protection of our constitutional system of government, [and] the advancement of the United States interests around the globe."[140] Harold Lasswell, one of the twentieth century's leading sociologists and political scientists, defined National Security very narrowly, focusing on military readiness and foreign powers saying "the distinctive meaning of national security is freedom from foreign dictation. National security policy implies a state of readiness to use force if necessary to maintain national independence."[141]

Others have defined national security as focusing on the importance of maintaining a society and a way of life. "A nation has security," [Walter] Lippmann wrote in June 1943, "when it does not have to sacrifice its legitimate interests to avoid war and is able, if challenged to maintain them by war."[142] Others, drawing on Lippmann's arguments have claimed "national

138 Sidel, Mark. More Secure, Less Free? Antiterrorism Policy & Civil Liberties after September 11. Ann Arbor, Michigan: University of Michigan Press, 2004. at 24.

139 *Katz v. United States* 389 U.S. 347 (1967) at 476.

140 President George W. Bush, National Security Presidential Directive 1, "Organization of the National Security Council System," February 13, 2001.

141 Walter Lippmann, U.S. Foreign Policy: Shield of the Republic, at 50-51 (Boston: Little, Brown, 1943).

142 Baker, James E. In the Common Defense: National Security Law for Perilous Times. New York: Cambridge University Press 2007at at 17.

security is measured by the advancement of certain societal values as well as security."[143] James E. Baker argues that even with the numerous definitions there are certain common themes that exist among them:

> Notwithstanding the absence of a common definition of national security, common themes are evident. Most definitions include an element of physical security, or freedom from coercion, both for the individual and the state. Most definitions also reference the preservation of a value system (e.g., "way of life").[144]

Application of these common themes, however, depends a great deal on the context, including who is defining National Security, what is going on in the world, and how one views important values. Baker argues, "where values are directly invoked (human rights) or indirectly invoked (way of life), these definitions are inherently subjective."[145] The effect of context on the definition of national security extends to the Executive and Legislative Branches. As Baker claims "the reality is that the executive branch employs and Congress creates different definitions for different purposes."[146]

4.11 Clash

Unfortunately, the meaning of national security has often led to power abuses by all three branches of government. These power abuses are evident throughout American history. It is often during war or times of national threat when liberty and constitutional guarantees have faced off against national security and have lost. These are the points in history when our government has overlooked the civil rights and liberties that they are bound by the Constitution to preserve.

> All of this has roots in our history: episodes of resurgent government control and historical moments of the threat of restriction on the exercise of our basic freedoms of speech and assembly; discriminatory treatment against aliens and

143 Ibid.

144 Ibid., at 19.

145 Ibid., at 19.

146 Ibid., at 18.

> immigrants, particularly in times of national tragedy or difficulty; increased surveillance of citizens and noncitizens and persecution of political dissent.[147]

In light of American history, James Baker argues:

> Through the Constitution comes the rule of law, an expectation that each branch of government, and each person within each branch, will comply with its structural, substantive, and procedural requirements and that the other branches will verify that this is done. This was not always so and there is nothing automatic about it remaining so.[148]

The realities of the post-September 11th world we live in has the potential of once again resulting in the rolling back of certain civil liberties. I first provide historical evidence of the loss of civil liberties during times where there were threats to National Security and then I explain how certain aspects of the Patriot Act and other governmental action make future abuse more of an assurance than a possibility.

From the very foundation of the United States, national security and civil rights have been in constant conflict, with each generation having to decide for themselves how they will resolve this clash. Often, the presence of peace came with abundant liberties while during times of war these liberties would fade. The first example of this was during the early stages of the nation when there was fierce conflict between the federalist and antifederalist parties. In an attempt to determine how to structure the nation Congress passed the Sedition Act of 1798, which "criminalized political criticism of the new U.S. government and led to a number of convictions of political opponents of the Federalist Party, which had sponsored the act."[149] This act limited the ability of citizens to speak freely about their government and voice their opinion, a right that some have argued is necessary in any democratic government.

---

147 Sidel, Mark. More Secure, Less Free?: Antiterrorism Policy & Civil Liberties after September 11. Ann Arbor, Michigan: University of Michigan Press, 2004. at 4.

148 Baker, James E. In the Common Defense: National Security Law for Perilous Times. New York: Cambridge University Press 2007at 21.

149 Sidel, Mark. More Secure, Less Free?: Antiterrorism Policy & Civil Liberties after September 11. Ann Arbor, Michigan: University of Michigan Press, 2004 at 4.

During the civil war, the government again limited constitutional liberties under the order of President Lincoln, who "sought to employ the military to maintain order in the North and to end the rights of citizens to challenge their detention through filing writs of habeas corpus. Under his orders, the Union army arrested thousands of nonmilitary citizen personnel, an action approved by Congress during the war."[150] This continued until 1866, when the Supreme Court stepped in to stop the abuse of authority.

Limitations on civil liberty did not only occur during times when there was internal battle and dissent. Similar limitations occurred when the nation was involved in a war or police action beyond its borders. For example, in World War I Congress passed the Espionage Act of 1917 under which

> U.S. residents could be jailed for speaking, printing, writing, or publishing any "disloyal, profane, scurrilous, or abusive language" about the U.S. government or causing, inciting, or attempting to cause or incite "insubordination, disloyalty, mutiny, or refusal of duty" in the Military.[151]

This time, Congress's action met with approval by the Supreme Court, who held that "[freedom of speech] does not … protect a man from an injunction against uttering words that may have all the effect of force' and that such circumstances are justified 'when a nation is at war [because] many things that might be said in times of peace are such a hindrance to its effort that their utterance will not be endured."[152] With the backing of other branches of government Congress went on to continue and intensify the effect of the Espionage Act of 1917 by passing the Sedition Act of 1918.

During WWI the government went beyond simply restricting the speech and expression of its citizens and also initiated forced detention of thousands of noncitizen residents during the

150 Chang, Nancy, Silencing Political Dissent: How Post-September 11 Anti-Terrorism Measures Threaten Our Civil Liberties (New York: Seven Stories Press, 2002), 22-23, 37-38.

151 Sidel, Mark. More Secure, Less Free?: Antiterrorism Policy & Civil Liberties after September 11. Ann Arbor, Michigan: University of Michigan Press, 2004 at 5.

152 *Schneck v. U.S.*, 249 U.S. 2, 120-21 (1866).

"Palmer Raids" in 1919. One of the disturbing aspects of these raids was the attempt by the government to distort the facts to appease the citizens.

> Pains were taken to give spectacular publicity to the raids, and to make it appear that there was great and imminent public danger… The arrested aliens were in most instances perfectly quiet and harmless working people. More than five hundred were forced out of the country, "not one of whom was proved to pose a threat to the United States.[153]

Twenty years later, during escalating conflict between the Soviet Union and the United States, and in direct response to the gradual growth of progressive left wing groups and unions, the Federal government again justified limiting individual liberty through the passage of the Smith Act of 1940. This act was strikingly similar to the Espionage and Sedition Acts. Under the Smith Act it was illegal to ""knowingly or willfully advocate, abet, advise, or teach the duty, necessity, desirability, or propriety of overthrowing or destroying any government in the United States by force or violence' or 'organiz[ing] … any… assembly of persons who teach, advocate, or encourage the overthrow or destruction of any government in the United States by force or violence."[154] The Smith Act was approved by the Supreme Court when challenged and it wasn't until 17 years later that the Court reversed the convictions. Two years later during World War II came perhaps the most infamous act of power abuse by the United States government with the commencement of Japanese Internment. During this period

> Over one hundred thousand American residents of Japanese origin, most of them U.S. citizens, were detained and interned in the western and southwestern United States beginning in 1942 under an executive order issued by President Roosevelt. In a time of international conflict and domestic emergency, a compliant Congress declined to challenge this blatant use of racial classifications to deny protection of the law to a particular group. And the Supreme Court upheld the executive branch's order against an appeal by a Japanese American Fred Korematsu, who had been charged and convicted with resisting detention and internment.[155]

153 Sidel, Mark. More Secure, Less Free?: Antiterrorism Policy & Civil Liberties after September 11. Ann Arbor, Michigan: University of Michigan Press, 2004at 5 – 6.

154 Chang, Nancy, Silencing Political Dissent: How Post-September 11 Anti-Terrorism Measures Threaten Our Civil Liberties (New York: Seven Stories Press, 2002), 22-23, 37-38.

155 Sidel, Mark. More Secure, Less Free?: Antiterrorism Policy & Civil Liberties after September 11. Ann Arbor, Michigan: University of Michigan Press, 2004 at 6-7.

The Supreme Court also upheld the conviction of Gordon Kiyoshi Hirobyashi who challenged Japanese Internment and curfews.[156]

Perhaps the most recent governmental power assertions during times of war prior to September 11th were the actions of the government during the Cold War, McCarthy era and the Vietnam War.

> The Cold War and McCarthy periods stands as perhaps the most widespread use of law to suppress disagreement and punish dissenting citizens and noncitizens in recent American history… In the McCarthy era, member of Congress and a Congressional committee, the House Un-American Affairs Committee, took the lead in repressive tactics. Not that the executive branch was passive: some of the key mechanisms of the Cold War and the McCarthy era-such as federal investigations, loyalty oaths, surveillance, and other tactics-depended heavily on surging executive power.[157]

During this time the Executive and Congress relied on the power of the FBI and other government organizations and agencies to implement these techniques.

> These government activities took a number of forms, but among the most well known was an FBI-wide counterintelligence and antiactivist program known as COINTELPRO. The program went far beyond research or the building of intelligence files - it was intended to "expose, disrupt, misdirect, discredit, or otherwise neutralize" civil rights, women's, trade union, and antiwar organizations and individuals affiliated with them, beginning in the mid-1950's and extending until the early 1970s. [158]

It wouldn't be for another twenty years after implementing this program that Congress would know its full repercussions, repercussions that still effect citizens today.

4.12 History Repeats itself: September 11th and its Aftermath

Following the devastating events of September 11th, 2001 it appears that history is once again repeating itself. The United States Patriot Act, as discussed in chapter one, was signed into law on October 26th, 2001, a mere 45 days after September 11th. This rapid action resulted in an

156 *Hirabyashi v. United States* 320 U.S. 81 (1943) and *Korematsu v. United States* 323 U.S. 214 (1944).

157 Sidel, Mark. More Secure, Less Free?: Antiterrorism Policy & Civil Liberties after September 11. Ann Arbor, Michigan: University of Michigan Press, 2004 at 7.

158 Sidel, Mark. More Secure, Less Free?: Antiterrorism Policy & Civil Liberties after September 11. Ann Arbor, Michigan: University of Michigan Press, 2004 at 8.

inadequate Congressional review of the Patriot Act's potential ramifications prior to its passage.[159] This act drastically shaped the laws surrounding intelligence gathering and investigation tools. While promising to better unite the efforts of government and aid in the prevention of terrorism, this act came with numerous limitations on liberty. Along with the Patriot Act came secret "sneak and peak" searches, increased electronic surveillance techniques, harsher treatment of noncitizens, detentions of citizens and noncitizens, secretive governmental action and numerous other changes. The Patriot Act also redefined terrorism and means in a broad and controversial manner.

> The Patriot Act enlarged the laws countering terrorism to provide for a new crime of "domestic terrorism," under which a range of law enforcement agencies could conduct investigations, surveillance, wiretapping, and other actions against organizations and individuals in the United States. The new offense was defined broadly to include "acts dangerous to human life" intended to "influence the policy of the government by intimidation or coercion." And even providing assistance to such a group- without any involvement in direct "terrorist activities"- may trigger prosecution under the act. The breadth of this definition of domestic terrorism has been the subject of substantial controversy.[160]

The Patriot Act has also severely affected non-citizens residing in America and abroad. The Patriot act has authorized several measures for how these individuals should be treated during this time of national unrest. A few of the newly created measures include: immigration and interrogation sweeps, detention without right to attorney or right to bond, deportation, bans from returning, mandated registration and denial of asylum.[161] The mandated registration was particularly criticized because of its "haphazard nature" and it was likened to "singling out Jews during the Nazi era."[162]

Of course the most pertinent impact of the Patriot Act for my discussion is the FBI's use of increased electronic surveillance through the expanded National Security Letter authority and

159 Ibid., at 9.

160 Ibid., at 11.

161 Ibid. 16 – 18.

162 Human Rights First (Lawyers Committee for Human Rights), Assessing the New Normal: Liberty and Security for the Post-September 11 United States (2003), 19.

through section 215 searches, which enabled the government to conduct searches similar to those conducted under National Security Letters in regards to foreign nationals.[163] Congressional expansion of FBI National Security Letter authority enables broad searches into the lives of both Americans and non-Americans which can be triggered by many things. According to Mark Sidel, "even speech activities, such as political statements or materials read can trigger this sort of largely unrestricted surveillance and information order."[164]

The broad effect of the Patriot Act has had a dichotomy of responses over the past seven years. These responses have included government efforts to praise the work and potential of the Patriot Act and grassroots attempts to warn others of its potential downsides. One of the claims made by Attorney General John Ashcroft exemplifies the government's perspective on the Patriot Act at the time of its passage.

> In the words of Attorney General John Ashcroft, the act "provides[s] the security that ensures liberty… First it closes the gaping holes in our ability to investigate terrorists. Second, the Patriot Act updates our anti-terrorism laws to meet the challenges of new technology, and new threats. Third, the Patriot Act has allowed us to build an extensive team that shares information and fights terrorism together."[165]

The claims that Ashcroft makes have been strongly opposed by grassroots organizations who have argued that these positive intentions may be starkly different than the realities of the Patriot Act's effect on American citizens and the government structure that we have come to rely on.

> In the words of the American Civil Liberties Union (ACLU), the act was "an overnight revision of the nation's surveillance laws that vastly expanded the government's authority to spy on its own citizens, while simultaneously reducing

163 Sidel, Mark. More Secure, Less Free?: Antiterrorism Policy & Civil Liberties after September 11. Ann Arbor, Michigan: University of Michigan Press, 2004 at 12 The Patriot Act also permits law enforcement authorities to obtain medical financial, student, computer, and other personal records from "third party" holders of those records under section 215, without notice to the target of the investigation, without explicitly tying the search to terrorism or spying, by recourse to the semisecret Foreign Intelligence Surveillance Court.

164 Ibid., at 13.

165 Ibid., at 10.

> checks and balances on those powers such as judicial oversight, public accountability and the ability to challenge government searches in court."[166]

This dichotomy however, has not slowed the government's desire to continue and even further enhance the security structure established by the Patriot Act. The government has continuously attempted to expand their authority through statutory and policy changes.

> Virtually since the moment the Patriot Act was enacted, there had been rumors that the Justice Department wanted more powers available to use against suspected terrorists and their supporters in the United States and that the attorney general and the White House would press quickly for authority in the event of another significant terrorist event, if not before.[167]

This is especially disturbing as terrorism is a constant threat that can never really fully be erased but just severely postponed. According to James Baker, this threat means that if we value our physical safety we must remain in that state of "continual effort and alarm attendant on a state of continual danger" that James Madison described and feared."[168] The problems that arise from this continual state of threat is the fact that

> There is danger that in facing this threat, presidents and their lawyers may conclude that (1) the process due is no process at all; (2) that every search or seizure is reasonable and (3) that extraordinary circumstances negate the necessity for meaningful checks and balances on the presidents use of the military and intelligence instruments.[169]

This concern has been validated over time in the actions of legislators and policy makers. Baker argues that "when faced with a choice between the concrete necessity of security and the abstract preservation of "liberty," policymakers tend to choose security."[170] I argue that in these decisions and in their deliberations these policymakers should not lose sight of the value of privacy.

---

166 Ibid.

167 Ibid., at 30.

168 Baker, James E. In the Common Defense: National Security Law for Perilous Times. New York: Cambridge University Press 2007at 10.

169 Ibid.

170 Ibid., at 22.

4.2 Privacy

Privacy is such a broad and subjective concept and perhaps one of the most important values to protect. The importance of privacy is evidenced by the vast attention paid to it each year. For as Fred H. Cate claims

> Privacy is the subject of thousands of scholarly and popular books, articles, position papers, reports, internet web pages and discussion groups, and newsletters. The debate over privacy protection has spawned an astonishing array of industry and academic conferences, working groups, public interest and lobbying efforts, public surveys, and news stories.[171]

The problem is defining exactly what "privacy" is. In an attempt to do just this Ken Gormely studied the privacy laws in the United States and in doing so he identified several understandings of privacy. First, privacy is "an expression of one's personality or personhood, focusing on the right of the individual to define his or her essence as a human being."[172] Second, according to Louis Henkin, privacy is "autonomy - the moral freedom of the individual to engage in his or her own thoughts actions and decisions."[173] Third, privacy lies in a "citizens' ability to regulate information about themselves, and thus control their relationships with other human beings" as argued by Alan Westin and Charles Fried.[174] Fourth, Ruth Gavison uses the "essential components" approach" to privacy. In this approach "scholars identify certain essential components such as "secrecy, anonymity and solitude" (Ruth Gavison).[175] While these four understandings are all unique, according to Fred H. Cate they are clearly intertwined:

> The information an individual chooses to disclose about herself under the third definition of privacy above focusing on control over information will certainly reflect upon the personality or identity that she chooses to portray, thereby implicating the first concept of privacy. The fear of compulsory disclosure may

171 Cate, Fred H. Privacy in the Information Age Washington D.C.: Brookings Institution Press, 1997. at 1.

172 Gormley, Ken. One Hundred Years of Privacy *Wisconsin Law Review* (September-October 1992), pp. 1337-38.

173 Ibid.

174 Ibid.

175 Ibid.

> very well influence her freedom to engage in independent action, thereby implicating the second concept of privacy. In short, more than one of these understandings may undergird a claim to privacy.[176]

This interconnectedness exemplifies the importance of privacy not only in defining who we are as individuals but the way that we interact with society. While these four understandings do not exemplify all the ways that privacy has been defined, they help to show the diversity of understandings of privacy For my discussion I primarily draw on the definition posited by Alan F. Westin in his study *Privacy and Freedom.* According to Westin, privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[177] This definition is the most applicable for viewing the types of searches that National Security Letters authorize the FBI to conduct.

While a right to privacy is not explicitly stated in the constitution, many Supreme Court cases have drawn on a right that they have justified through numerous interpretations of the text of the constitution. One of the earliest discussions of a constitutional right to privacy was presented by Samuel D. Warren and Louis D. Brandeis in their Harvard Law Review article *The Right to Privacy*. Since that time an implicit right to privacy has been cited in numerous Supreme Court cases and has been the turning point for several. One of the most prominent cases establishing the existence of a right to privacy was *Griswold v. Connecticut,* a case surrounding the use of contraceptives where Justice Douglas argued that there is a right to privacy that can be found implicit in the penumbra of the First, Third, Fourth, Fifth, and Ninth amendments of the Bill of Rights.[178] The type of privacy found in this decision, and later implemented in the famous abortion case *Roe v. Wade*, is much broader than the privacy that the Fourth Amendment has been defined to protect. This type of privacy is more often defined as individual autonomy.

---

176 Cate, Fred H. Privacy in the Information Age Washington D.C.: Brookings Institution Press, 1997. at 19.

177 Westin, Alan F. Privacy and Freedom. New York: Atheneum, 1967 at 7.

178 *Griswold v. Connecticut* 381 U.S. 479 (1965) at 484 .

A right to privacy has been referenced in several Fourth Amendment cases as well, including: *Boyd v. United States*, 116 U.S. 616, which describes the Fourth and Fifth Amendments as protecting against all government invasions of 'the sanctity of a man's home and the privacies of life'; and *Mapp v. Ohio* ,367 U.S. 643, which referred to the Fourth Amendment as creating a 'right to privacy, no less important than any other right carefully and particularly reserved to the people.'[179] A right to privacy has also been argued as implicit within the fourteenth amendment's protection of liberty.[180]

4.21 Context

Many have argued that while privacy is important it cannot be properly defined without taking into account the context in which it is being defined. Fred H. Cate argues that "the specific meaning of any understanding of privacy… is determined almost entirely by the context in which it is derived and applied."[181] Based on this reasoning privacy can be affected not only by the circumstances in which it is discussed but also by who is discussing this value within a particular context. This is exemplified above in the differing opinions held by the Attorney General and the ACLU on the Patriot Act. This context contingency however, is an especially important consideration now as we are faced with a continuous state of national threat and a seemingly unending War on Terror.

While the Bill of Rights was designed to protect the rights of citizens regardless of the circumstances, the reality is that "where some may have though such constitutional principles were fixed, they may yet come unhinged under the pressure of indefinite threat."[182] This is especially important to consider in light of uncertainty that we will ever leave this time of insecurity. For as James Baker contends, we run the risk that there will never be a full return to

179 Ibid.

180 Ibid.

181 Ibid.

182 Baker, James E. In the Common Defense: National Security Law for Perilous Times. New York: Cambridge University Press 2007 at 31.

peace to restore the "constitutional equilibrium" and for that reason we must remember that "changes in constitutional interpretation today may persist past tomorrow. Thus, assertions of constitutional authority may serve, in effect, as silent and sometimes secret constitutional amendments."[183]

4.24 Costs of Privacy

It is also important to remember that there is not an absolute value in privacy. There is an implicit battle between the costs of adding privacy protection and the costs of losing our privacy. By adding privacy protections we risk hindering investigations by slowing them down however, by giving up privacy protections we risk having our very autonomy taken from us. For as Charles Fried argues, privacy is important not only in an individual's ability to keep others out but it is important in giving people the ability to choose who to share their information with and to what extent. Privacy protection is also important in protecting the liberty that we enjoy. For as Fried argues:

> Besides giving us control over the context in which we act, privacy has a more defensive role in protecting our liberty. We may wish to do or say things not forbidden by the restraints of morality, but which are nevertheless unpopular or unconventional. If we thought that our every word and deed were public, fear of disapproval or more tangible retaliation may keep us from doing or saying things which we would do or say if we could be sure of keeping them to ourselves or within a circle of those who we know approve or tolerate our tasks.[184]

Allowing the government to seize and analyze information from many diverse sources threatens the type of privacy needed to protect exactly this type of liberty. For this reason, the cost and value of privacy must be considered within this balance between privacy and national security for each investigation type and tool.

183 Ibid., at 10.

184 Fried, Charles. "Privacy " Yale Law Journal, Vol. 77, No. 3 (Jan., 1968), pp 475-493 at 485.
,

4.3 National Security Letter Balance

When the national security that National Security Letters afford is weighed against the value of privacy in the information that they authorize the FBI to obtain I argue that equilibrium has not been reached by the current NSL provisions. In order to justify this argument I try to answer two questions. First, to what extent do National Security Letters limit an individual's privacy claims over their information and second, is the national security that these letters afford worth this loss?

As mentioned in earlier chapters, National Security Letters currently can reveal a vast amount of broad information on individuals, information in which there is a reasonable expectation of privacy. This expectation of privacy is not protected by the way that the FBI handles and disseminates this information, as discussed in chapter three. Essentially, the government has taken away an individual's control over their information and has taken upon itself the right to claim this information and do with it as they please. This action by the government completely negates the privacy, as defined by Charles Fried and Alan Westin, in this information that an individual holds.

The national security that these letters afford is not worth this cost. Out of over 200,000 National Security Letter requests the government has only provided evidence of one terrorism conviction resulting in part from information obtained through a National Security Letter[185]. The details surrounding this case and conviction are so concealed that it is impossible to know the extent that National Security Letters aided in this conviction. It is also important to note that it is not clear what crime the individual committed or was attempting to commit and therefore it is impossible to know how broadly terrorism was defined in this case. As discussed above, terrorism has been very broadly defined by the Patriot Act. Even if these letters played a substantial role in securing this conviction, this victory for the government must be viewed in light of the thousands

185 Barton, Gellman. ""The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans." The Washington Post, November 6, 2005. at AO1.

upon thousands of innocent individuals searched. This result can be likened to finding the proverbial needle in the haystack. This haystack is made of the records on individuals that the FBI creates and increases constantly through its broad "fishing expeditions" into the lives of Americans and non-Americans alike.

National Security Letters fail to provide the benefits of potential deterrence, as they currently are so heavily cloaked in secrecy. Those who are investigated under the FBI's NSL authority are, for the most part, unaware that this search ever took place. The most that the American population is made aware of at this point in time is that National Security Letters exist, they are used to obtain diverse and private records, and they may be challenged by the recipient. It would appear that arguably the only deterrence effect would be of deterring a potential terrorist from using certain forms of communication, or using the internet without encrypting their searches and data. National Security Letters fail to provide the typical deterrence formula of: if you do x the result is y, x being an action and y being a National Security Letter investigation. This is in part due to the broad definitions offered by the government for certain statutory terms and the lack of consensus on what these terms should mean. National Security Letters afford the government one thing: speed. In fact, one could argue that the type of deterrence that occurs is the type that Charles Fried argues threatens liberty. The government's ability to access thousands of records, analyze them, and control who they disseminate these records to threatens an individual's ability to freely act and speak and can potentially have a severe chilling effect. This seems especially plausible with the fact that Americans cannot be certain that their records will not be searched.

By expediting the FBI's national security and clandestine intelligence investigations these NSLs authorize the FBI to get around the purposely cumbersome system of checks and balances within our federal government. The Founding Fathers, being quite aware of the potential for power abuse, designed a system of checks and balances in order to assure that one branch could not usurp complete authority and to provide for the protection of the civil rights that America's

constitutional government is bound to protect. The cumbersome nature of the American federal government is evidenced in many ways including: the existence of numerous veto points in the legislation process, Congress' ability to limit the President's Commander-in-Chief authority through its power of the purse, the power of judicial review, and in the appointments to the Judiciary made by the executive only upon the approval of the senate. These processes do not result in a government of expediency, however, they result in a government whose authority is balanced to ensure that invasions of constitutional rights and liberties are prevented or at least minimized.

The FBI's complete discretion over whom to investigate, when to investigate them, and to what extent lacks the necessary checks and balances to ensure that constitutional protections are afforded to every individual. Through their expansion of the National Security Letter provisions, Congress authorized the FBI to vigorously investigate terrorism and intelligence by expanding their investigation methods. Having been elected to represent their constituents and to protect their constitutional rights, these Congressmen were undoubtedly aware of the Fourth Amendment's prohibition of unreasonable searches. Based on this reasoning it would appear that Congress expected the FBI to be dedicated to their investigations while simultaneously acting in a detached and neutral manner to ensure that their searches were reasonably construed, a seemingly impossible expectation. For these reasons, National Security Letter provisions, as they currently exist, fail to protect an individual's reasonable expectation of privacy and are therefore unconstitutional on Fourth Amendment grounds.

4.4 Recommendations

The current National Security Letter provisions of the ECPA, RFPA, FCRA and NSA must be reconsidered in light of this failure and that there must be certain procedural safeguards added to them. Determinations on whether a National Security Letter search is reasonable should not be left in the sole hands of the FBI. In order to ensure that an individual's privacy is protected there must be multiple layers of protection added to National Security Letter provisions. First,

National Security Letter searches must be approved by a neutral magistrate outside of the FBI prior to the letter being sent. During this approval stage the judge must determine first if there is a prior finding of probable cause, or at the very least a finding of individualized suspicion, as to give the FBI reason to search the individual or individuals in question. Second, the judge must determine what the appropriate parameters of the search should be based on the FBI's recommendation and the specific circumstances of each case. Third, a judge must ensure that these parameters are expressly stated and delivered along with the national security letter.

Following the search a judge should ensure that the search was completed in compliance with the request. Finally, there must be the addition of an after the fact notice requirement which notifies any individuals whose information has been searched and who have been removed from the FBI's suspect list that a search of their records occurred, that the search was approved by a neutral magistrate, and the grounds on which the search was justified. As I argue in chapter three these individuals should then be able to challenge these letters on Fourth Amendment Grounds if they feel that it was unreasonable and this required notification will enable them to do so. The addition of a neutral magistrate's prior approval and prior determination of the parameters of the search will help to ensure that those who may never be removed from the FBI's suspect list are still guaranteed that any search of their records is judicially authorized and limited to the least intrusive means and that their Fourth Amendment rights are ensured.

While the current National Security Letter provisions are unconstitutional, Congress can create a more constitutionally acceptable National Security Letter by implementing these above recommendations. This Congressional change will ensure that there can be no question as to the existence and extent of these requirements. The FBI would then be forced to adhere to these proposed standards for all National Security Letter searches. A Congressional revision of the NSL provisions will ensure that there is the potential for judicial reconsideration of these terms as to their extent and will provide a standard for the judiciary to base their determinations on the validity of a National Security Letter search.

4.42 Exceptions Considered

Prior to September 11th 2001 there existed a wall between terrorism/intelligence investigations and criminal investigations and a wall between investigations of foreign nationals and investigations of American citizens. These walls affected many aspects of legal considerations from whether an individual should have standing to challenge a claim, and whether there should be particular leniencies during certain exigent circumstances. As these factors often greatly affected the result, I address both of these considerations and I argue that these distinctions should not substantially alter the recommended procedure.

4.42 (a) Terrorism and Intelligence v. Criminal Investigations

Terrorism and intelligence cases have become very difficult to distinguish from criminal investigations as a result of the new legislation in two main ways. First, there is now, as mentioned above, a new much broader definition of terrorism which includes the broad term "domestic terrorism," violations of which can include criminal acts done even without the intent of terrorism. For example, "acts dangerous to human life" can include anything from battery to serial murder which are acts that can be tried under current criminal law. Second, the FBI's dissemination of National Security Letter information sometimes includes, as mentioned above, taking this information to the district attorney's office for them to determine if there is a criminal act for which their suspect may be tried through proper legal procedure. This makes it very difficult to determine whether there is a criminal or terrorist act, or potentially even both, for which a suspect is being tried.

In fact, even prior to September 11th the Supreme Court was asked to decide whether a national security investigation should merit an exception from Fourth Amendment procedure. In their 1972 decision in *U.S. v. U.S. District Court*, the Supreme Court held that domestic security is a vague concept and for that reason there exists room for potential abuse.

> Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee

> political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment.[186]

This statement is evidence that there has always been a difficulty in determining whether a case should be considered an intelligence investigation or a criminal investigation, however, regardless of the distinction the Fourth Amendment still applies, for as Justice Brennan argues in his *Katz v. United States* concurring opinion:

> Spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers… there is so far as I understand the constitutional history no distinction under the Fourth Amendment between types of crime…Article III s. 3 gives treason very narrow definition and puts restrictions on its proof…But the Fourth Amendment draws no lines between various substantive offense.[187]

For these reasons I argue that there should be no exception to the above recommendations based on whether the crime at issue was regarded as terrorism.

4.32 (b) Foreign Intelligence Exception

The second exception is one when the target of an investigation is a foreign national or noncitizen. In the past there has been a vast amount of deference to the executive branch when a foreign agent or power was the target of an investigation. I argue that the Patriot Act has blurred the line between foreign nationals and American citizens to a practically indistinguishable level. This blurring is evident in the changes made to National Security Letter provisions which do not distinguish in the type of search they conduct based on who is being targeted. This blurring also exists in the changes made to other federal statutes such as the statute which creates the Foreign Intelligence Surveillance Court (FISC), a court originally created through the Foreign Intelligence Surveillance Act (FISA) detailing the procedure that must be followed for investigations of foreign nationals. In 2001, the Patriot Act changed the requirements for conducting investigations under the minimal standards of the FISC by saying that the purpose of the investigation no longer had to be to investigate foreign agents or powers so long as that is a significant purpose.

186 *United States v. United States District Court* 407 U.S. 297 (1972) at 320.

187 *Katz v. United States* 389 U.S. 347 (1967) at 507.

In *Mayfield v. United States,* the district court held that FISA standards have been applied so broadly as to allow American citizens to be tried. According to the district court, "[w]here a "United States person"--a citizen or a permanent resident alien-- is involved, the definition of an "agent of a foreign power" requires, in most instances, a showing of criminal activity.[188] Based on the history of abusing this blurred distinction and the difficulty in determining exactly who should be classified as a foreign agent or power, my recommendations should be applied to every National Security Letter search regardless of the target.

4.5 *Concluding Remarks*

Drawing on existing case law, scholarly opinion, abuse of authority noted in the Inspector General's audit, current Congressional actions, and the existence of factors distinguishing National Security Letters from any other type of investigatory tool, I contend that the current National Security Letter provisions are unconstitutional on Fourth Amendment grounds. I have justified this conclusion by examining the Fourth Amendment and the limited applicability of the current precedent to National Security Letter searches. I argue that to correct the existing deficiencies, current NSL provisions must be amended by Congress to include three procedural safeguards: prior approval by a neutral magistrate, the addition of a warrant requirement specifying the parameters of the NSL search, and a prior finding of probable cause.

As I have argued, there exists a valuable right to privacy that has been recognized by numerous scholars and the judiciary. Unfortunately, in light of the horrific events of September 11th, the federal government has continuously whittled away at privacy seemingly without contention. In order to prevent sliding down the proverbial "slippery slope" to a Big Brother type of government such as that depicted in George Orwell's 1984, I argue that it is imperative that Americans challenge this abused authority while we are still able to. This is imperative for as Judge Marrero claims in his decision in *Doe v. Ashcroft*

188 *Mayfield v. United States* WL 2792447 (2007) at 5.

> Sometimes a right, once extinguished, may be gone for good. Few satisfying means may then be available to truly restore to the particular victim or to the larger society the value of the loss.[189]

Americans must ensure that in enabling the government to protect the nation's security we are not forced to give up the civil rights and liberties that our government is constitutionally bound to protect.

189 *Doe v. Ashcroft* 334 F.Supp.2d 471(2004) at 477.