

Table of Contents

Introduction	2
Chapter 1 “A History of Electronic Surveillance and the Right to Privacy”	5
Early History of Government Surveillance.....	5
The Beginnings of a Constitutional Right to Privacy.....	7
The Right to Privacy Emerges.....	11
“A Reasonable Expectation of Privacy”.....	12
The Beginnings of Executive Wiretapping: The FDR Precedent.....	15
The Birth of the National Security Agency and the FBI’s Rampant Wiretapping...	19
The Church Committee and Operation SHAMROCK.....	21
United States v. United States District Court.....	24
The Foreign Intelligence Surveillance Act.....	26
Chapter 2 “Modern Electronic Surveillance Practices and Policies”	28
The PATRIOT Act.....	28
The Beginning of the Terrorist Surveillance Program.....	31
The Program Leaks.....	35
The Legal Defense and Changes to the Program.....	36
The Protect America Act of 2007.....	37
Recent Developments of the Program.....	43
Chapter 3 “The Mechanics of the Terrorist Surveillance Program”	45
The Mechanics.....	45
Government Data Mining Before 9/11: Carnivore.....	49
Government Data Mining After 9/11.....	50
The Cooperation of Telecommunication Companies.....	56
National Security Letters.....	61
Chapter 4 “The Constitutionality of the Terrorist Surveillance Program”	65
The Doe Cases.....	65
It Does Not Belong to You.....	69
The Curious Case of Pen Registers.....	63
Finding a Reasonable Expectation of Privacy.....	76
An Important Means to an End.....	80
Jackson’s Test.....	84
The Supremacy Argument.....	86
The FDR Precedent Revisited.....	88
An Ambiguous AUMF Argument: The Last Hope.....	89
The Verdict.....	91
Conclusion.....	92
Appendix.....	96
Works Cited.....	99
Acknowledgements.....	104

Introduction

In the last thirty years, the world has shrunk. In 1980, if you wanted to speak to a friend, you would either have to meet in person or wait until you got home (or a phone booth) to give them a call; if they weren't home, you were out of luck. Today, you can call or text message on a cellular phone, email them from either a phone or computer, write on their wall on Facebook, send them a "tweet" on twitter, chat through a instant messaging service like America Online Instant Messenger, video chat with them on Skype, meet them in a video game server and play a game together, or still call them using a regular phone. In short, we have become a nation online.

This not only applies to personal communication but to professional communication as well. Almost any business transaction requires a computer and some form of network. For example, any bank transaction or a doctor visit requires exchanging very personal information. Additionally, many companies and banks allow customers to pay bill online. The last decade also brought in the era of online shopping with online auctions sites such as eBay.com and online discount sites such as Amazon.com. In addition, virtually all existing retailers have launched online. To say the least, it appears much of what we buy, how we communicate, and how we live is somewhere on a computer.

While a digitalized world may be more convenient to use, it is also makes it more convenient to obtain personal information. Before the electronic age, the Fourth Amendment to the United States Constitution would require a federal agent to get a warrant from an independent judge before obtaining personal information. The Fourth Amendment guarantees:

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

The Fourth Amendment has traditionally protected individuals from unreasonable government searches. With the rise of electronic communication, the Supreme Court slowly applied the Fourth Amendment to non-physical searches such as wiretaps. The Court nor Congress, however, have been able to keep pace with the rapid technological change of the last thirty years.

The Bush Administration, however, recognized the rapid change. Shortly after the attacks of September 11, 2001, President George W. Bush authorized the National Security Agency and the Federal Bureau of Investigation to begin a massive electronic surveillance program to prevent future terrorist attacks. Merely a month after the attacks, FBI and NSA agents approached telecommunication companies, financial institutions, and private data brokers for information on millions of people, foreigners and Americans, within the United States. The goal of the program was not only to intercept communications, but also to establish a massive database that could determine possible attacks from interpreting patterns of data. In order to amass this massive database, the NSA and FBI demanded customer information from corporations and financial institutions.

The controversy of the program, however, was that it violated a clear statute regulating this type of surveillance. The Foreign Intelligence Surveillance Act, created shortly after President Richard Nixon's own domestic electronic surveillance activities, set clear authorization procedures in certain cases of electronic surveillance targeted at foreign powers. President Bush, however, believed his powers as commander-in-chief, as written in Article II in the US Constitution gave him the authority to ignore this statute in order to protect the nation. Many legal scholars and Congressmen, however, argued that the President had no such authority to

execute such an invasive program. President Bush's legal scholars, however, presented a different view of Presidential power that would allow the unilateral authorization of the program.

The Terrorist Surveillance Program, while ultimately directed at terrorist suspects, implicates millions of Americans. This project will explore two important Constitutional questions: whether the program violated the Fourth Amendment's protection from warrantless searches and wiretap and whether the President had the Constitutional authority to authorize such a program in the face of clear Congressional opposition.

Chapter 1

“A History of Electronic Surveillance and the Right to Privacy”

Electronic surveillance is not a Fourth Amendment issue according to a strict reading of the Amendment. Originally, the Fourth Amendment only applied to physical searches of property. The birth of electronic communications changed this, however. No longer did people have to wait to talk to each other in person, they could simply pick up a telephone; the federal government decided to listen in. Government officials could do so because a telephone conversation was not property according to the Fourth Amendment at the time. However, legal scholars in the late nineteenth century believed that a government search went beyond walking onto property. The legal community pushed for a new interpretation of the Fourth Amendment that would protect citizens from unwanted government intrusion; the courts slowly followed suit. The new technology presented innovative opportunities to prevent and prosecute crime. The government quickly and often used wiretaps to listen in to conversations to catch criminals in the act. After time of unregulated snooping, however, the courts, Congress, and the American people had enough.

Early History of Government Surveillance

The history of government surveillance begins long before the electronic surveillance or even the Constitution. There is evidence that the colonists sought protection from any type of eavesdropping or unwarranted snooping. Early eavesdropping laws emerged from English common law during the early days of the American colonies. The Crown also adapted its privacy laws for the colonies' postal delivery system (Diffie and Landau, 2007, p. 144). Despite this,

however, the Crown established a “secrets office . . . whose staff routinely opened correspondence that the government considered potentially subversive” (Diffie and Landau, 2007, p. 145).

In response the Crown’s surveillance, Congress added a provision in the Postal Act of 1792—the Act that established the United States Postal Service—that prohibited the opening of mail unless it were deemed undeliverable. Despite this, the law had to be amended in the Postal Act of 1825 ,because of reports of spying from all levels of government. The new law prohibited opening other people’s mail by *anyone*; the spying of mail, however did not stop (Diffie and Landau, 2007, p. 145). This snooping activity ballooned during the Civil War, under President Lincoln’s continual extra-Constitutional acts to save the Union. While it was allowed during the time, the Supreme Court would eventually rule that first class mail could not be opened without a warrant – which required a government official to show a magistrate that they had probable cause a suspect is or had committed a crime -- in Ex Parte Jackson (1878) (Diffie and Landau, 2007,p. 146). This ruling is the first to give Fourth Amendment protection to a form of communication.

As the telegraph, became a vital tool during the Civil War, the US government tried to tap it for information and surveillance. Along with the invention of wired communications came a new world of government surveillance (Bellis, 2010, para. 6). The telegraph created two new opportunities to eavesdrop: “one could tap the wire or one could read the message later from copies kept at telegraph companies . . . the latter search was preferred by the government;” similarly, one-hundred forty years later, Internet storage became a preferred method of surveillance. The government seized control of the telegraph lines during the Civil War and seized copies of all telegrams sent within a twelve-month span and censored any telegraph

message coming from Washington, D.C. (Diffie and Landau, 2007, p. 146). The courts nor Congress has spoken on the legality of government seizure of stored communications.

The Beginnings of a Constitutional Right to Privacy

Nor did the courts or Congress prohibit wiretapping. Originally, the Fourth Amendment only protected unreasonable searches and seizures. At time of the Constitutional Convention, there were only two forms of communication: verbal communication and mailings. Surveillance of the former required a government official to be present for the conversation; in this case, the individuals could evade eavesdropping by entering a private place. Surveillance of the latter, of course, was prohibited by the Postal Act of 1789 and eventually the Fourth Amendment in Ex Parte Jackson (1878). The emergence of electronic communication, however, forever changed Fourth Amendment searches. For the first time, electronic communication allowed the government to obtain information that normally be obtained through a physical search or through a confession through interrogation.

By the late nineteenth century the change in communication technology spurred worry about the government's wiretapping abilities. Legal scholars Louis Brandeis and Samuel Warren, in the Harvard Law Review article "The Right to Privacy," believed that a world with electronic communication required Constitutional interpretation. Rather than limit the Fourth Amendment to physical searches, Brandeis and Warren (1890) argue that implicit in the Constitution is "the right to be left alone." They write, "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'" Brandeis and Warren argue that common law practices have guaranteed that an individual has "the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall

be communicated to others.” They believe that the Fifth Amendment’s protection against self-incrimination proves this point (Brandeis and Warren, 1890). It would be 150 years before the Supreme Court adopted a Constitutional right to privacy and a few more before privacy became a bedrock principle of the Fourth Amendment.

Brandeis and Warren’s “The Right to Privacy” was a revolution in the legal world, but it was not the first mentions of a right to privacy in a Supreme Court case. Justice Joseph Bradley’s majority opinion in Boyd v. United States (1885) is one of the first declarations of a right to privacy in the Supreme Court. The case struck down a Federal act that forced defendants to surrender illegally imported merchandise; if they refused to surrender the evidence, they were forced to sign a confession to their accused crimes (p. 617-618). The Court cited not only a violation of the defendant’s Fifth Amendment rights against self-incrimination, but also the defendant’s Fourth Amendment rights from unreasonable search and seizure. Bradley asserted that “compulsory production of a man’s private papers to establish a criminal charge against, or to forfeit his property, is within the scope of the Fourth Amendment” (p. 622). Later in the opinion, Bradley makes an interesting note on the essence of what the Fourth Amendment protects:

It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offense (p. 630).

While it may fall short of declaring a Constitutional right to privacy, this influential statement would fuel one of the most important dissents in Supreme Court history.

In Olmstead v. United States (1928), the petitioners were convicted of conspiracy to violate the National Prohibition Act “by unlawfully possessing, transporting and importing intoxicating liquors and maintain nuisances, and by selling intoxicating liquors” (p.455). Evidence obtained during this case came from a wiretap, installed without prior judicial approval; the wiretap consisted of

“small wires . . . inserted along the ordinary telephone wires from the residences of four of the petitioners and those leading from the chief office. The insertions were made without trespass upon any property of the defendants. They were made in the basement of the large office building. The taps from house lines were made in the streets near the houses (p. 457).

In a five-to-four majority, the Court upheld the legality of the wiretap. In the majority opinion, Chief Justice William Howard Taft ruled that because the wiretap was not actually installed on the property it could not be considered a Fourth Amendment search. Because Government officials did not actually trespass on the defendant’s property to install the wiretap, no search occurred (Olmstead v. United States, 1928, p.465). Furthermore he asserted that a warrant was unnecessary for wire tapping because a warrant “must specify the place to be searched and the person or *things* to be seized” (p.464). Taft finally ruled that “the language of the [Fourth] Amendment cannot be extended and expanded to include telephone wire reaching to the whole world from the defendant’s house of office” (p. 465). Taft and the other four justices took a literal interpretation of a property; for them, the Fourth Amendment only protected an individual from an unwarranted physical search of his or her property.

Justice Brandeis, on the other hand, did not take such a restricted view of the Fourth Amendment. He argued for a more expansive reading of the Fourth Amendment:

Legislation, both statutory and Constitutional, is enacted, it is true, from an experience of evils, but its general language should not, therefore, be necessarily confined to the form that evil had theretofore taken. Time works changes, brings into existence new conditions and purposes (Olmstead v. United States, 1928, p.472-473).

Brandeis implied that it would be ridiculous to limit the Fourth Amendment to Eighteenth century standards. In those days, “force and violence were then the only means known to man which a government could directly affect self-incrimination . . . [or] secure possession of his papers and other articles incident to his private life” (p. 473). Brandeis, in an eerie prediction, warned that if the Court failed to adapt to changing technology there may come a time when the government “without removing papers from secret drawers, can reproduce them in court” without a warrant (p. 474).

Telephone lines, Brandeis asserted, deserved Constitutional protection because it is a medium in which intimate secrets could be unwillingly discovered. Brandeis, believed that Ex Parte Jackson was an applicable precedent because like a telephone call, “[the] sealed letter entrusted to the mail [service]” is similar to the telephone’s “public service” to transmit calls (Olmstead v United States, 1928, p. 475). He noted that unlike the mail, the “the tapping of one man’s telephone [may lead to the tapping] of every other person whom he may call or who may call him” (p. 476).

Finally, Brandeis made an impassioned plea for the Court to accept some form for a right to privacy:

The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They conferred, as against the Government, the right to be let alone – the most

comprehensive of rights and the right most valued by civilized men. To protect that right, *every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means, employed, must be deemed a violation of the Fourth Amendment* (Olmstead v United States, (1928), p. 477-478) [emphasis added].

The Court in Olmstead did not accept Brandeis's logic, but the Court would adapt his famous dissent in less than forty years.

The Right to Privacy Emerges

In that case, Griswold v. Connecticut (1965), Estelle Griswold, the Executive Director of the Planned Parenthood League of Connecticut in New Haven, Connecticut and C. Lee Buxton, the physician at the same facility, were arrested for violating the state's prohibition of giving contraception advice and tools to a married couple; they were both fined \$100. In the majority opinion, Justice William O. Douglas declined to rule based on existing precedents and instead looked to rule based on an implicit Constitutional right to privacy (Griswold v. Connecticut 1965, p. 482). He cited a number of cases to chart out this new right. Douglas cited, among other cases, NAACP v. Alabama in which the Court ruled that the state of Alabama could not force the NAACP to disclose its members lists because it was a restraint on their "freedom to associate and [to keep] privacy in [their] associations" under the First Amendment. Justice Douglas wrote, "the First Amendment has a penumbra where privacy is protected from governmental intrusion" (p. 383).

Justice Douglas believed that this hidden right to privacy was beyond the penumbra of the First Amendment. He wrote that the Constitutional right to privacy was protected by:

The Third Amendment in its prohibition against the quartering of soldiers “in any house” in time of peace . . . The Fourth Amendment [which] explicitly affirms the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. [And] The Ninth Amendment [which] provides: “The enumeration in the Constitution, of certain right, shall not be construed to deny or disparage others retained by the people” (Griswold v. Connecticut 1965, p. 515).

The Court thus ruled that the Connecticut law infringed on the married couples’ right to privacy from unwanted government intrusion.

Justice Arthur Goldberg, agreed with Justice Douglas that there is a Constitutional right to privacy, but he differed in where he believed that right was located. In the beginning of his concurring opinion in, he believed that the Ninth Amendment alone contained the implicit right to privacy (Griswold v. Connecticut 1965, p. 487). He noted that James Madison worried that the Bill of Rights would “disparage those rights which were not placed in that enumeration [of the first eight amendments]. Madison, thus, introduced the Ninth Amendment which read, “The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people,” to protect from potential abuse. (p. 489, qtd. Galses and Seaton (1834) I Annals of Congress 439). Out of this evidence, Justice Goldberg would find it hard to believe that the right of intimate and privacy of marriage, “a relation as old and as fundamental as our entire civilization,” would not be an inherent right of the people not to be disparaged by unwanted government intrusion (p. 496). While this decision did not strike down or affect the standing of the Olmstead precedent, it did make way for a ruling that would.

“A Reasonable Expectation of Privacy”

Two years later, the court official rejected Olmstead. That case, Katz v. United States, accomplished two things: it legitimized the a Constitutional right to privacy and applied privacy to Fourth Amendment jurisprudence. In Katz v. United States (1967), the government charged the defendant with transmitting wagering information from a pay telephone in Los Angeles. During the trial, the government entered evidence that was obtained from an “electronic listening and recording device” installed and maintained by the FBI (p. 348). The district court allowed the evidence to be entered into court because the evidence was not obtained from a search recognized by the Fourth Amendment according to the Olmstead precedent. On appeal, the Ninth Circuit Court of Appeals upheld the decision because “there was not physical entrance into the area occupied by the petitioner” (Katz v. United States 1967, p. 349).

Mr. Katz petitioned the Supreme Court to determine whether the FBI violated his Constitutional right to privacy and his Fourth Amendment rights from unreasonable search and seizure by invading his “Constitutionally protected area” within the booth. Justice Potter Stewart, a dissenter in Griswold, however, declined to grant Fourth Amendment protection to a phone booth; Stewart wrote the Fourth Amendment “protects people, not places” (Katz v. United States 1967, p. 351). Furthermore, he argued that:

the Fourth Amendment cannot be translated into a general Constitutional ‘right to privacy.’ That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all (p. 350).

Based on this previous Fourth Amendment jurisprudence, the Government argued that Mr. Katz had no expectation of privacy because he was in a glass-encased booth that could be visible from the outside. Justice Potter argued:

But what [Mr. Katz] sought to exclude when he entered the booth was not the intruding eye – it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less that an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment (Katz v. United States, 1967, p. 352).

Justice Stewart realized that the telephone had become an important part of everyday private communication. He believed that recent decisions such as Griswold have “eroded” the principles of the Olmstead ruling and could no longer be considered controlling precedent (Katz v. United States, 1967, p. 353). Stewart ruled that wiretapping a telephone was considered a search that is protected by the Fourth Amendment (p. 387). Thus, according to Fourth Amendment jurisprudence, prior authorization from a magistrate had to be granted before that search could be conducted (p. 358).

Justice John Marshall Harlan II agreed with the ruling for the most part, however, he believed that the Court should allow some exceptions for the warrant in government electronic surveillance cases (Katz v. United States, 1967, p. 362). First, and most notably he held that “a person has a constitutionally protected reasonable expectation of privacy” and that expectation of privacy must be recognized as reasonable by society (p. 360, 361). In other words, under Harlan's test, not all private conversations were protected by the Fourth Amendment. For example, speaking about a crime knowingly in front of a police officer in a police station obviously has not expectation of privacy; on the other hand, an intimate conversation over the

phone in a private area would likely be considered a Constitutionally protected private talk. Harlan's "reasonable expectation" test became controlling precedent in cases such as Smith v Maryland (1979) (p. 747), Kyllo v United States (2001), (p. 32), and California v. Ciraolo (1985), (p. 211), among others. Unlike Stewart's majority opinion, Harlan's concurring opinion actually gave government officials a clear test to determine whether a search may be conducted.

The Beginnings of Executive Wiretapping: The FDR Precedent

The Katz ruling allowed for a national security exception; however, presidents had been conducting national security wiretaps for years. Most notably, it began with President Franklin Roosevelt. FDR and later President George W. Bush believed their powers as commander-in-chief and diplomat-in-chief, proscribed in Article II of the Constitution, granted them the authority to protect the nation from foreign attack. FDR and Bush often cite United States v. Curtiss-Wright Export Co. (1936) as evidence of their power to do anything to protect that nation from *foreign* attack (United States House of Representatives (Part I) 2007, p.33). That decision stated the President is the "sole organ of the nation in external relations" and that Congress could not interfere with that Constitutional right (United States v. Curtiss-Wright Export Co. 1936, p. 319). Presidents have believed the "sole organ" in addition to their roles as commander-in-chief granted them the authority to use wiretaps on foreign targets (even if Americans are implicated) to prevent attacks.

This notion was uncontroversial after the Olmstead decision. That is until the passage of the 1934 Communications Act. The Olmstead ruling sparked controversy around the nation. *The New York Times* blasted the decision saying, "Prohibition, having bred crimes innumerable, has succeeded in making the Government the instigator, abettor and accomplice of crime. It has now

made universal snooping possible.” (Caplan and Katyal 2008, p.114). In response, Congress outlawed eavesdropping on private telephone lines. Section 605 of the Communications Act states:

No person receiving . . . or transmitting . . . any interstate or foreign communication by wire or radio shall divulge or publish the . . . contents . . . thereof, except through the authorized channels of transmission or reception, to any person other than the addressee (Caplan and Katyal , 2008, p. 115).

It is important to note that while the intention of the law might be implicit, the actual wording of the law does not forbid wiretapping communications *per se*. The law only forbids the *divulging* of the content of communications and not the actual listening. President Franklin Roosevelt’s Department of Justice accepted a similar interpretation of the law (Caplan and Katyal , 2008, p. 116).

The Supreme Court questioned this discrepancy between Congress and the FDR administration in a series of famous cases. In Nardone v United States (Nardone I) (1937), the appellant, Mr. Nardone, questioned the admissibility of evidence against him that was discovered through a warrantless wiretap under the 1934 Communications Act. In the Second Circuit appeal hearing, Judge Learned Hand believed that the Olmstead precedent controlled this case because the Act was “silent as to the admissibility of messages intercepted contrary to its provisions” and that “Congress did not see fit to adopt the suggestion of direct legislation to make such evidence inadmissible” (Caplan and Katyal 2008, p.118). The Supreme Court, however, overturned the Second Circuit’s ruling:

The plain words of section 605 forbid anyone, unless authorized by the sender, to intercept a telephone message, and direct in equally clear language that ‘no person’ shall

divulge or publish the message or its substance to ‘any person’ (Caplan and Katyal 2008, p. 120).

It would seem clear-cut that the Supreme Court had settled the controversy.

The FBI and the Department of Justice, however, interpreted the Nardone I case differently. FBI director J. Edgar Hoover and Attorney General Robert Jackson “interpreted the Nardone decisions to mean that it was unlawful to both ‘intercept’ *and* ‘divulge’ communications, and had decided that it was not unlawful to intercept communication as long as the contents were kept within the federal government” (Caplan and Katyal 2008, p. 179). President Roosevelt, himself, also accepted this loose interpretation, as he authorized the use of wiretaps under his authority against any “persons suspected of subversive activities against the government of the United States, including suspected spies” (p. 180). Thus, the Department of Justice and the FBI continued warrantless wiretapping until, the Supreme Court’s ruling in Nardone II in 1939.

After Nardone I, the US government continued to pursue the case against Mr. Nardone. In the remanded trial, the government introduced the content of the calls without admitting that they obtained the information from a wiretap. The district court found in favor of the government once again as did the Second Circuit court on appeal. The Supreme Court, however, once again ruled against the government. In his majority opinion, Justice Felix Frankfurter, admonished the government for taking such a “meticulous reading of technical language.” He goes on to criticize the government:

decent respect for the policy of Congress must save us from imputing to it a self-defeating, if not disingenuous purpose . . . to forbid the direct use of methods thus characterized but to put no curb on their full indirect use would only invite the very

methods deemed ‘inconsistent with ethical standards and destructive of personal liberty’(Caplan and Katyal, 2008, p. 124).

The Supreme Court finally ruled that the government could not wiretap a phone line without a warrant. It is important to note, however, that the Court ruled based on the 1934 Communications Act and not on the Constitutionality of warrantless wiretapping; the Olmstead ruling was still good precedent in Constitutional matters.

Despite the Court’s explicit ruling FDR believed there was an exception to the rule. FDR sent a confidential memo to Attorney General Robert Jackson that stated he did not believe that Nardone ruling applied to the “matters involving the defense of the nation.” FDR subsequently authorized wiretaps that involve national security:

The Attorney General could only authorize FBI wiretapping after an investigation of the need in each case, with wiretaps limited: (1) to a minimum number; (2) insofar as possible to aliens; and (3) by devices direct to the conversation (Caplan and Katyal, 2008, p. 128).

Jackson, and numerous scholars, disagreed with FDR however on this national security exception. In his memoir about his time in the Roosevelt administration, he wrote about the memo:

The only case that I recall in which [FDR] declined to abide by a decision of the Supreme Court was its decision that federal law enforcement officers could not legally tap wires. Wire tapping had been used in the Department of Justice by my predecessors. After the decision in *Nardone v. United States* came down in late 1939, I as Attorney General quickly issued an order to discontinue all use of the interception of wire communications . . . I had not liked FDR’s May 21, 1940 memorandum authorizing wiretapping as an

approach to the problem. It seemed to me that wire tapping was a source of real danger if it was not adequately supervised, and that the secret of the proper use of wire tapping was a highly responsible use in a limited number of cases, defined by law, and making wire tapping criminal outside of those purposes or limits (Caplan and Katyal 2008, p. 129).

Caplan and Katyal (2008) argue that Nardone II was straight forward in its interpretation of the 1934 Communications Act. The Court ruled “the plain words . . . forbid *anyone*, unless authorized by the sender, to intercept a telephone message and direct in *equally clear language* that ‘no person’ shall divulge or publish the message or its substance to any person” (p. 129). Despite the clear language of the act and the Nardone rulings, FDR continued with his warrantless wiretapping program, in the name of national security. This would not be the last time an executive would actively disobey Congress and the Supreme Court in the name of national security.

The Birth of the National Security Agency and the FBI’s Rampant Wiretapping

The Nardone rulings created legal barriers for government agencies from gathering information from an electronic source without a warrant. While the 1934 Communications Act prevented the same thing, President Franklin Roosevelt’s national security exception allowed the government to side step the will of Congress. After President Roosevelt’s death, President Harry Truman created an agency to carry out the intelligence monitoring of electronic communications; this new entity was called the National Security Agency.

Truman created the NSA in October 1952 in an effort to reorganize and strengthen communications surveillance. Congress confirmed the establishment of the Agency in 1959 and designated it as the principal agency for electronic intelligence gathering (United States Senate,

1976, p. 7). The National Security Agency, though, would not be the only agency to conduct wiretapping. The NSA merely joined the FBI and the CIA in the electronic surveillance of foreign entities and US citizens.

After the World War II, FBI director Herbert Hoover sought to keep the wiretapping authority granted under President Roosevelt. Hoover succeeded and expanded his wiretapping authority when he sought renewal from President Truman. He tricked President Truman by deleting the sentence (without informing the president) in the original authorization memo that limited wiretapping and directed it “insofar as possible to aliens.” The FBI could now spy on Americans without a warrant. Truman approved the memo without knowing the change. Even when he did discover the change in policy, Truman did nothing to limit the new authority (Diffie and Landau 2007, p. 181).

The FBI’s newfound power of wiretapping led to some of the most notorious domestic spying cases in American history. The FBI, under Hoover, is believed to have wiretapped senators, Congressmen, Supreme Court Justices, and political figures “without any pretense of investigating criminal activities (Diffie and Landau, (2007), p. 185). In the 1960’s, President John Kennedy, used the FBI’s wiretap program to spy on political opponents and several journalists. President Lyndon Johnson used wiretaps less liberally, but did accept information gathered on Martin Luther King Jr. and Congressional opponents to the Vietnam War.

The rampant warrantless wiretapping irked many in Congress. In an effort to curb wiretaps, Congress passed the Omnibus Control and Safe Streets Act. Title III of the act created a detailed procedure for authorization to intercept wired communications:

The procedure requires the issuance of a judicial warrant, prescribes the information to be set forth in the petition to the judge so that . . . he may find probable cause that a crime

has been or is about to be committed. It requires notification to the parties subject to the intended surveillance within a period not more than ninety days after the application for an order of the period of the extension of the order. . . . The Act contains a saving clause to the effect that it does not limit the Constitutional power of the President to take such measures as he deems necessary to protect the nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities (United States Senate, 1976, p. 70).

While the law did somewhat curb excessive wiretapping, it did not stop the practice. President Nixon famously used wiretaps often; he justified the wiretaps as matters of national security. The Omnibus Crime Control and Safe Streets act of course allowed this exception and in fact endorsed it as an inherent Presidential power. President Nixon used the FBI's wiretaps to collect information on reporters and White House officials whom he believed leaked information about the secret bombings in Cambodia (United States Senate, 1976, p. 163). Many also accused the Nixon administration for using warrantless surveillance "on leaders of the anti-war movement, black movements, Catholic activist pacifists, and advocates of youth culture" (Quint 1981, p. 21). Wiretaps also became the center of controversy when individuals paid by the Committee to Re-Elect the President attempted to install wiretaps in the Democratic National Committee headquarters at the Watergate Hotel (Diffie and Landau 2007, p. 199-200).

The Church Committee and Operation SHAMROCK

In reaction to Nixon's use of warrantless wiretaps, a special Congressional committee began investigating the history of executive wiretapping. The Senate Select Committee to Study

Governmental Operations with Respect to Intelligence Activities (commonly known as the Church Committee) began its investigation in January 1975 (Diffie and Landau 2007, p. 200). The Committee uncovered many abuses of wiretapping (much of which is sighted in this project) since the 1934 Communications Act and the Nardone rulings that supposedly prohibited warrantless wiretapping. The Committee ultimately concluded:

Too many people have been spied upon by too many government agencies and too much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on the behalf of a foreign power. The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone “bugs,” surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens (Diffie and Landau 2007, p. 201).

One of the abuses The Church Committee spent a considerable time was a program called “Operation SHAMROCK.” According to the United States Senate (1976):

SHAMROCK was the cover name given to a message-collection program in which the Government persuaded three international telegraph companies . . . to make available in various ways certain of their international telegraph traffic to the U.S. Government. For almost 30 years copies of most international telegrams originating in or forwarded through the United States were turned over to the National Security Agency and its predecessor agencies (p. 58).

The program, created sometime before or during World War II, was used widely to collect foreign intelligence to help the war effort. During the war, all foreign messages went through the

wartime censorship program. The Department of Defense sought renewal of the program in 1947 after the war. The representatives of the three telegraph companies involved agreed to cooperate as long as “they would suffer no criminal liability and no public exposure” (United States Senate, 1976, p. 58). The Bush Administration would similarly push for immunity for telecommunication companies who cooperated in the Terrorist Surveillance Program.

The arrangement between the telegraph companies and the government allowed the NSA to search through international telegrams for international targets. Two of the companies, RCA Global and ITT World Communications, handed over a large bulk of its international messages to NSA personnel who were allowed to sort through it themselves. The other company, Western Union, sorted through the telegrams itself and only handed over information relevant to foreign targets. In the early 1960s, telegraph companies began saving telegraphs on magnetic tapes and then turning them over to the NSA. This change in technology allowed the NSA to screen those international telegraphs for American citizens placed on a watch list to be further analyzed by NSA agents or have that information passed on to other government agencies (United States Senate, 1976, p. 59).

The NSA, sorted through about 150,000 messages a month; a few thousand of these were distributed to other agencies. Only a few executive officials knew of the highly confidential Operation Shamrock. According to testimony, “no President since Truman had been informed of [Operation Shamrock].” Due to growing controversy of the operation, Secretary of Defense James Schlesinger terminated SHAMROCK on May 15, 1975 (United States Senate, 1976, p. 60). Operation SHAMROCK provided the impetus for the Church Committee to push for a change in America’s foreign surveillance laws. It is interesting to note that another NSA

program, much like SHAMROCK, would be implemented in communication companies shortly after September 11, 2001.

United States v United States District Court

Two important events in the 1970s would curb the executive's excessive use of warrantless wiretapping. One of the events, the Supreme Court's ruling in United States v United States District Court, finally gave a definitive answer to whether the a warrant was necessary for purely domestic wiretaps regarding national security.

In United States v United States District Court (1972), the United States convicted three individuals with conspiracy to destroy government property. One of the defendants, Mr. Plamondon was charged with the bombing of a CIA office in Ann Arbor, Michigan (p. 299). During the trial, the government introduced evidence obtained from warrantless wiretaps. The Attorney General believed a warrant was not necessary because the wiretaps were used "to gather intelligence from information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government" (p. 300). The District Court, however, disagreed and ruled that the wiretaps violated the defendant's Fourth Amendment rights. The Government appealed the ruling, but the Court of Appeals of the Sixth Circuit upheld the decision that the wiretaps violated the Fourth Amendment (p. 305).

The Supreme Court recognized that was the first occasion the Court has confronted intelligence surveillance in domestic matters. (United States v. United States District Court, (1972), p. 299). Congress legislated the use of wiretaps in the 1934 Communications Act and in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, but Congress had either

actively or inactively allowed the President to make exceptions in national security cases (p. 301). The government argued that Congress recognized the President's Constitutional authority in national security matters. Justice Powell, however, ruled that the act merely "left Presidential power where it found them" (p. 303) Powell cited Senator Phillip Hart's speech on the Senate floor about the national security exception in Title III:

In addition, Mr. President, as I think our exchange make clear, nothing in section 2511 (3) even attempts to define the limits of the President's national security power under present law, which I have always found extremely vague . . . Section 2511 (3) merely says that if the President has such a power, then its exercise is in no way affected by title III (qtd. by Justice Powel p. 306).

This proved to the Court that Congress had no intention of granting the President additional powers of domestic surveillance. The ruling, then, had to focus on whether the President had the inherent Constitutional authority to authorize these domestic wiretaps.

The Court limited the ruling only to domestic surveillance, because the Court recognized the President's power to conduct foreign surveillance, affirming the "sole organ" doctrine of Curtiss-Wright (United States v United States District Court (1972), p. 308-309). Rather, the case addressed a question left open in Katz v United States: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving national security" (Katz v United States p. 358, qtd. by Justice Powell p. 309).

The Court ultimately ruled that Katz must be applied to domestic surveillance even in national security cases in order protect basic Constitutional protections. Powell noted that the judicial warrant is an important matter in Fourth Amendment protection because "these Fourth Amendment freedoms cannot properly be guaranteed if domestic surveillance may be conducted

within the discretion of the Executive Branch” (United States v. United States District Court, 1972, p. 317). Furthermore, the independent nature of the judiciary is a “time-tested means of effectuating Fourth Amendment rights . . . [even] post-surveillance review would never reach the surveillances which failed to result in prosecutions (p. 318). Powell rejected the argument that a judicial warrant could complicate confidential matters involving targets because the courts can “recognize that domestic surveillance involves different considerations from the surveillance of ‘ordinary crime’” (p. 320). For these reasons, the Supreme Court unanimously ruled that prior judicial review is needed in all types of domestic surveillance “and that approval may be made in accordance with such reasonable standards as the Congress may prescribe” (p. 324).

The Foreign Intelligence Surveillance Act

Congress let the Court’s ruling in United States v United States District Court, stand in matters of domestic surveillance. Six years after the ruling, however, Congress cleared the messy area of foreign surveillance.

The Foreign Intelligence Surveillance Act was the first time Congress attempted to regulate the President’s power to collect foreign surveillance. With FISA, Congress created the Foreign Intelligence Surveillance Court (FISC) to ensure that American’s civil liberties would be protected without comprising national security. The court would be comprised of seven federal district judges appointed by the Chief Justice of the Supreme Court. In order to obtain a warrant from the Foreign Intelligence Surveillance Court (FISC), a government official had to prove to a FISC judge that they had probable cause that the evidence in question would prove that the foreign target was committing a crime. FISA allowed the Attorney General to issue an emergency authorization, but the government had to apply for FISC review within seventy-two

hours. FISA also clarified that at least one of the targets had be of foreign descent or was in a foreign location; domestic targets required the government to go to a traditional court to obtain a warrant based on probable cause. (Foreign Intelligence Surveillance Act, 1978).

FISA and the United States v United States District Court ruling attempted to rein in the expanding ability of the Executive branch to gather intelligence. The rapid changes in technology from the 1890s to the 1970s created a new area in Constitutional law. Conversations that would normally be conducted in a private could now be broadcasted to the unwanted ear. The Executive Branch saw the emergence of telecommunications as a new means of crime control and a tool to prevent foreign attacks. While Congress and the Courts attempted to limit the executive's wiretapping, Presidents often claimed that it was their Constitutional duty to harness the new medium to protect the nation. While the United States District Court ruling and FISA attempted to solve these questions, an even quicker revolution in technology would once reawaken this constitutional debate.

Chapter 2

“Modern Electronic Surveillance Practices and Policies”

September 11 changed everything. As many times as that phrase has been said, it is true. The attacks of September 11, 2001 made terrorism America’s next big enemy after the end of the Cold War. This new war on terror required the US government to adapt and implement the latest technology and methods to save American lives; unlike the Cold War, however, the enemy could blend into the general populous. In order to fight this war, the United States had to be able to quickly and effectively collect and process intelligence both overseas and at home. The challenge for the Bush administration, however would be whether their efforts to protect the nation could adhere to its laws.

The PATRIOT Act

The public wanted an answer to the attacks quickly. Congress and the President worked quickly to update security laws -- one of them the Foreign Intelligence Surveillance Act -- in order to meet the need of the new era. The Bush Administration put a considerable effort to get a bill quickly through Congress. The Justice Department drafted an initial bill, that dramatically expanded executive powers, some which had been previously rejected in Congress as “unnecessary infringements on civil liberties” (Foerstel, 2008, p. 30). In fact, the Justice Department became extremely involved in the drafting process of the Patriot Act.

On September 19, 2001, the White House invited key senators and representatives to discuss the Justice Department’s draft of the Patriot Act. According to Forestel (2008), the draft of the Patriot Act:

was severe, calling for such things as indefinite detention of any noncitizen who may 'further or facilitate acts of terrorism.' . . . [permitted] eavesdropping data throughout the government, permitted Internet service providers to allow the FBI to tap e-mail, and lowered the FISA standard for surveillance authority. The members of Congress, including Sen. Patrick Leahy [D-VT], worked on a compromise version of the Justice Department's draft. Leahy reached a compromise with a representative of Attorney General John Ashcroft that the government could not use "illegally obtained evidence against U.S. citizens and that a court must review information before it was shared among intelligence and law enforcement agencies (p.33)

The compromise between Congress and the administration would not last long.

Shortly after the meeting however, Ashcroft said the deal was off. Leahy was forced to accept [the original Justice Department draft of the bill] because he knew that the bill would not pass Congress without the Justice Department's approval. Ashcroft had the power to do this because if he did not publicly approve of the bill, then it would seem that Congress was limiting the President from effectively fighting terrorism, which would be politically disastrous for Leahy and Congress in a time of crisis (Foerstel, 2008, p.33).

Once the bill made it to Congress, the leaders of the House and Senate feverishly tried to push the bill as fast as possible. Republican leaders wanted unanimous consent of the Justice Department draft of the bill as did Sen. Tom Daschle, the Democratic leader in the Senate. The lack of debate about the bill worried Senators Leahy, Russ Feingold (D-WI), and Arlen Specter (R-PA). Specter wrote Leahy a memorandum about his concerns: "in recent decisions, the Supreme Court of the United States has declared acts of Congress unconstitutional when there has been an insufficient record or deliberative process to justify the legislation" (Foerstel, 2008,

p. 35). Specter pressed Leahy for meaningful hearings on the bill, but Leahy worried that opening the bill to amendments would only make it more prone to infringements on civil liberties. The majority leader, Tom Daschle, agreed and pushed for unanimous consent on the Justice Department draft (p. 37). Senator Russ Feingold was the only senator who opposed the bill, but Daschle pleaded Feingold to let the bill pass for now (p. 36).

Congress passed the “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001” on October 26, 2001 or a little more than five weeks after its introduction in the House (United States House of Representatives, 2009, p. 12). For the most part, the law updated existing statutes. For instance, Section 206 of the Patriot Act allowed Roving “John Doe” Wiretaps. Roving wiretaps, as opposed to conventional wiretaps record conversations on one person’s multiple communication devices. Roving wiretaps were created to track dealers began using temporary disposable cell phones, commonly known as “burners,” which allowed them to change telephone numbers easily. This made it difficult to track criminals, because traditional wiretap procedures required a new warrant for a new telephone number. The Patriot Act allowed the targets receiving the wiretaps to be concealed in an open court for national security purposes (United States House of Representatives, 2009, p.91).

Section 209 allowed the government access to stored communications. “The Patriot Act amended criminal statutes so that the government can obtain opened emails and emails older than 180 days with only a subpoena instead of a warrant” (United States House of Representatives, 2009, p. 91). Traditionally, information stored on telecommunication servers, such as the emails of subscribers, required a judicial warrant based on probable cause. This change, however, made the process of obtaining stored communications much easier by

completely eliminating judicial oversight. A subpoena differs from warrant because it did not require judicial approval. Rather than a search of suspect's property, subpoenas are targeted at either companies that hold information about targets or individuals that hold information about a target. The Supreme Court has ruled subpoenas only require a government agent to show that the documents would be relevant to an investigation (Slobogin 2007, p. 144). Subpoenas were allowed the relaxed standard because they would not incriminate the entities that surrender the information. Furthermore, while that information may incriminate a target, they have no expectation of privacy of information that they voluntarily give to third parties (Slobogin 2007, p. 143). The Patriot Act dramatically expanded executive power in many ways including electronic surveillance. Now, the executive branch could unilaterally obtain personal information without judicial oversight. In the Information Age where most private data is handled electronically by third parties, this executive expansion had the possibility to affect millions of American.

The Beginning of the Terrorist Surveillance Program

The Bush administration began its electronic surveillance program, formally called the Terrorist Surveillance Program, shortly after 9/11. President Bush first formally authorized the domestic electronic surveillance program in October 2001; it is uncertain whether the authorization came after or before the Patriot Act was signed into law (Offices of Inspectors General, 2009, p. 11). The program was only authorized for "the inception of the content of communications into and out of the United States where there [is] a reasonable basis to conclude that one party to the communication [is] a member of al-Qa'ida or related terrorist organization" (p.1). The Terrorist Surveillance Program aimed to work within the confines of FISA by

targeting foreign targets; therefore, the Bush administration felt that it did not have to consult the Foreign Intelligence Surveillance Court for a warrant.

The program remains largely classified, but details released give the public some picture of the scope of the Terrorist Surveillance Program. From its inception, the President reauthorized the program every forty-five days. The NSA provided the technical expertise for the program and collected the actual information (Offices of Inspectors General, 2009, p.1). The NSA sent collected information to the FBI, CIA, the Office of the Director of National Intelligence (ODNI), and the National Counterterrorism Center (NCTC) for further analysis and investigation. The NSA also reportedly chose its own targets and did not seek approval from the Justice Department or the Bush administration (Lichtblau and Risen 2005, p. 4). The list included “American citizens, permanent legal residents, tourists and other foreigners” (Lichtblau and Risen 2005, p. 2). While the list contained American names, the administration forbade the NSA from collecting information on purely domestic-to-domestic communication without a warrant obtained from the Federal Intelligence Surveillance Court because of the clear precedent banning such surveillance in United States v. United States District Court case. (Lichtblau and Risen 2005, p. 3).

The Bush administration authorized all of this without consulting Congress. Sometime after the program started, Vice President Dick Cheney invited Congressional leaders from both parties to the White House to discuss the program along with NSA Director Lieutenant General Michael Hayden and CIA Director George Tenet; it is uncertain how much the Congressional leaders were told about the program (Lichtblau and Risen, 2005, p. 3). In fact, President Bush believed that he was not obligated to inform Congress; he did, however inform them when he felt the time was “[consistent] with national defense needs” (Offices of Inspectors General, 2009, p.

6). Furthermore, the Presiding Judge of the Foreign Intelligence Surveillance Court, Colleen Kollar-Kotelly, was the only member of the Court notified of the program from January 2002 to January 2006 (Offices of Inspectors General, 2009, p.17). The administration clung to the Office of Legal Counsel's view that the President had the Constitutional authority to authorize the program without prior approval from Congress or the FISC; this decision to not inform either entity, however, would be a costly political mistake.

The political firestorm began quietly within the administration before the public knew about the program. White House Chief of Staff Andrew Card and White House Counsel Alberto Gonzales approached the Office of Legal Counsel (OLC) for a new legal authorization of the program in early 2001. By this time a number of the original staff, including Yoo, had left the OLC. The OLC felt that the program relied too much on a loose reading of FISA and the President's Article II powers and felt uncomfortable reauthorizing the program (Caplan and Katyal, 2008, p.144). Attorney General John Ashcroft and Deputy Attorney General James Comey agreed with the OLC to not reauthorize the program. Shortly after, though, Ashcroft was hospitalized with a "serious illness." He transferred his powers to Comey while in the hospital. With Ashcroft in the hospital, Card and Gonzales decided to take advantage of the situation in order to re-authorize the program. Comey, however, caught wind of the plan before Card and Gonzales arrived. When they arrived, "they carried an envelope and explained to Ashcroft why they were there and why wanted him to approve the reauthorization of the [Terrorist Surveillance Program]" (Fisher, 2008, p. 299-300). Comey, under his authority as acting Attorney General, however, was able to prevent Ashcroft from re-authorizing the program. Many within the Justice Department threatened to resign after they learned of Comey's hospital encounter. President

Bush, however, averted a mass resignation by assuring Comey that they would not pressure the Justice Department until the program met legal standards (Fisher, 2008, p. 299-300).

It is apparent that many in the administration did not approve of the controversial program. A detailed explanation of the program follows in the next chapter, but this chapter warrants some discussion of the technical aspects of the program. The program obtained electronic data primarily in two ways: directly from telecommunication companies or indirectly through administrative subpoenas. The first way has limited first-hand accounts because the program is still largely classified. In Frontline: Spying on the Homefront, former AT&T technician Mark Klein noticed government agents were constructing a secret room in the company's San Francisco branch. Klein explained the purpose of the room: "So what they do with the splitter is they intercept that data stream and make copies of all the data, and those copies go down on the cable to the secret room" (Young, 2007). In short, the NSA blindly filtered information through a major telecommunications company to search for intelligence on suspected targets. The next chapter will explain these splitter rooms more comprehensively.

The other method, administrative subpoenas, called National Security Letters allowed the FBI to obtain the records from financial companies on targeted suspects. Section 505 of the Patriot Act expanded the use of the national security cases; the next chapter will explore the use and legality of National Security Letters more in depth. These administrative subpoenas obtain corporate records with the authorization of an FBI official; there is no judicial oversight. Furthermore, these corporations are gagged from revealing that they received a National Security Letters (Slobogin, 2007, p. 176). While National Security Letters were used before 9/11, its usage skyrocketed after 9/11. According to Nakashima (2010), "the Justice Department issued 192,500 National Security Letters from 2003 to 2006, according to a 2008 inspector general

report, which did not indicate how many were demands for Internet records.” An intergovernmental report found many possible abuses of National Security Letters and many issued without proper authorization (Slobogin, 2007, p. 176). The vast power of the program to conduct warrantless searches stirred controversy throughout the nation; the Bush Administration’s secret surveillance program would not stay secret for very long.

The Program Leaks

On December 16, 2005, *New York Times* reporters James Risen and Eric Lichtblau broke the news about the Bush Administration’s Terrorist Surveillance Program. According to Risen and Lichtblau (2005), “nearly a dozen current and former officials, who were granted anonymity because of the classified nature of the program, discussed it with reporters for *The New York Times* because of their concerns about the operation's legality and oversight.” Furthermore:

The White House asked *The New York Times* not to publish this article, arguing that it could jeopardize continuing investigations and alert would-be terrorists that they might be under scrutiny. After meeting with senior administration officials to hear their concerns, the newspaper delayed publication for a year to conduct additional reporting. Some information that administration officials argued could be useful to terrorists has been omitted (Risen and Lichtblau, 2005, p.1)

The *New York Times* published classified information—some of which is previously cited—about the creation of the program, how the program works, and the controversy it created within the Administration. Notably, the article goes into considerable depth about how the program did not obtain warrants despite:

The standard of proof required to obtain a warrant from the Foreign Intelligence Surveillance Court is generally considered lower than that required for a criminal warrant - intelligence officials only have to show probable cause that someone may be "an agent of a foreign power," which includes international terrorist groups - and the secret court has turned down only a small number of requests over the years (Risen and Lichtblau, 2005, p.3).

The article also noted that the NSA had little oversight when selecting targets. The lack of oversight created widespread controversy among leaders of the FBI and NSA as well analysts in the program. Some have stated that they "wanted nothing to do with the program" because they believe the program might be illegal. Because of concerns, the White House revamped elements of the program (Risen and Lichtblau, 2005, p.4).

The Legal Defense and Changes of the Program

On December 19, 2005, three days after the leak, President Bush held a press conference to discuss the program. President Bush defended the legality of the program stating:

As President and commander-in-chief, I have the Constitutional responsibility and the Constitutional authority to protect our country. So consistent with U.S. law and the Constitution, I authorized the interception of international communications of people with known links to al Queda (Young, 2007).

During the conference a reporter asked "and why did you skip the basic safeguard of asking courts for permission of these intercepts. Mr. Bush replied:

You're referring to the FISA court in your question. Of course we use FISAs. But FISAs is [sic] for long-term monitoring. What is needed in order to protect the American people is the ability to move quickly (Young, 2007).

It would appear that President Bush believed that the FISC, and FISA at large, was a mere formality that was inferior to Presidential authority.

Many legal authorities, including the administration's lawyers, asserted this very principle; in fact, some even argue that FISA infringes in the President's Constitutional powers. John Yoo, on November 2, 2001, wrote a memorandum stating that FISA—which “purports to be the exclusive statutory means for conducting electronic surveillance for foreign intelligence”—might infringe on the President's Article II powers as commander-in-chief to protect the nation. For Yoo

the ultimate test of whether the government may engage in warrantless electronic surveillance activities is whether such conduct is consistent with the Fourth Amendment, not whether it meets the standards of FISA, (Offices of Inspectors General, 2009, p. 11). Moreover, Yoo stated that when it comes to privacy arguments, the government's national security interests are more important than the individual's privacy interests (Offices of Inspectors General, 2009, p.13). Professor Robert Turner from the University of Virginia Law School believed that FISA has no Constitutional grounding. He cited Curtiss-Wright as evidence that the President is the ultimate authority in foreign surveillance (United States House of Representatives (Part I), 2007, p. 35). Indeed, President Jimmy Carter, upon signing the bill, acknowledged that FISA infringed on his Presidential duties. His Attorney General, in Congressional testimony stated, “the current bill recognizes no inherent power of the President to conduct electronic surveillance . . . *this does not take away the power of the President under the*

Constitution” (United States House of Representatives (Part I), 2007, p. 57 [emphasis included]).

Like Presidents before him, George W. Bush showed disdain for FISA’s limits on his perceived Constitutional authority; unlike other Presidents, Mr. Bush actually directly confronted FISA to pursue that Constitutional power.

Moreover, during the December 19, 2005 press conference, President Bush stated that he believed the Authorization to Use Military Force allowed him the authority to authorize the program. The statute, which states:

To authorize the use of United States Armed Forces against those responsible for the recent attacks launched against the United States. Whereas, on September 11, 2001, acts of treacherous violence were committed against the United States and its citizens; and Whereas, such acts render it both necessary and appropriate that the United States exercise its rights to self-defense and to protect United States citizens both at home and abroad; and Whereas, in light of the threat to the national security and foreign policy of the United States posed by these grave acts of violence; and Whereas, such acts continue to pose an unusual and extraordinary threat to the national security and foreign policy of the United States; and Whereas, the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States (“Authorization for Use of Military Force,” 2001).

The Bush Administration, believed that this broad authorization signified a Congressional concession of Presidential authority.

Critics of Bush’s legal logic, however pounced on flaws in the administration’s reasoning. Critics note that Yoo omitted an important provision in FISA that severely undermined his argument. Yoo believed FISA was not meant to apply to wartime because of the

President's power as commander-in-chief during wartime allows to take necessary measures to protect the nation. A section in FISA, however, grants the President fifteen days of warrantless wiretapping after a declaration of war; government agents were required to obtain a warrant after that period expired (Offices of Inspectors General, 2009, p. 12). This omission compromised his argument that FISA did not apply to wartime and thus his entire legal argument for sidestepping FISA (Offices of Inspectors General, 2009, p.20).

In addition, the Bush administration points to FDR's own experience with warrantless wiretapping. As mentioned in the previous chapter, FDR initiated wiretaps in the face of the 1934 Communications Act. The Justice Department points to FDR's action as evidence of strong precedent for Presidentially authorized surveillance (p. 104). Critics, however point out that FDR's warrantless wiretaps met considerable resistance from the other government branches and the public at large. While the 1934 Communications Act did not prohibit wiretapping *per se*, the Nardone cases clearly prohibited the government from *any* wiretapping without a judicial warrant (Caplan and Katyal, 2008, p. 105). Furthermore, critics point out that FISA, unlike the 1934 Communications Act, is very explicit about wiretapping. Basing Bush's program on the controversial FDR precedent provided little legitimacy for the program (p. 143).

The Protect America Act of 2007

Because the Bush Administration found it difficult to work within the current confines of FISA or even defend its legal position while avoiding FISA, the President decided it was time for a change. The Bush administration believed current surveillance law under FISA required necessary updates in order to effectively protect the country. One of the largest problems with FISA, for the Administration, was its lag with modern technology. At the time, FISA did not

require a warrant for wireless communication, such as a satellite communication. Technology, however, had changed considerably since the law passed 1978. The Justice Department complained that in 1978 most international communications were wireless satellite communications. Congress, evidently, wanted to leave foreign-to-foreign surveillance that took place out of the country to Presidential discretion. Local communications, on the other hand, were almost exclusively wired; today, the situation is reversed. Most international communications by 2007 were carried through wired communications like the Internet while most local communications were carried through wireless communications like cellular phones (United States House of Representatives (Part I), 2007, p.17). FISA's requirement for warrants on all wired communications thus prevented government agents from conducting purely foreign surveillance. This compromised the original purpose of FISA to only issue warrants that implicated foreign agents or American citizens within the United States.

The Protect America Act changed this problem in two ways. First, the law removed "electronic surveillance" from its definition of a search. Now, electronic surveillance conducted on a target reasonably believed to be outside of the United States did not require a warrant from the FISC (United States House of Representatives (Part I), 2007, p. 14). A warrant was still not needed for surveillance of any type on a foreign target, even if the target was communicating with an American citizen. In other words, a warrant was not required to intercept a conversation between an American and a foreign target (United States House of Representatives (Part I), 2007, p. 14). The Bush administration pushed for the term change, because of a FISA court ruling that determined that communication that passed through an Internet node in the US required a warrant even if both targets were located outside of the United States (Addicott and

McCaul, 2007, p. 64). The change created a clearer processes for authorization to monitor foreign communications.

Second, the Protect America Act created an authorization process between the Justice Department and the FISC. “, Section 105B of the Protect America Act, required the Attorney General to create a procedure to ensure that a target was outside of the United States (United States House of Representatives (Part I), 2007, p.18). If surveillance was conducted on someone within the United States without a warrant, the contents of that surveillance could be divulged or retained for 72 hours unless the Attorney General believed that the information implicated immediate danger, death, or bodily harm (United States House of Representatives (Part I), 2007, p.19). Foreign surveillance could be conducted without judicial approval, if it met guidelines to ensure that a target was outside the US (United States House of Representatives (Part I), 2007, p.155). This surveillance had to be renewed by the Attorney General after one year. The act also created a direct data link (such as the NSA splitter room) between communications companies and the government. This created a more stream-lined interception process (United States House of Representatives, (Part II), 2007, p. 21).

The Protect America Act dramatically expanded Presidential authority; it is thus not surprising that the bill met heated controversy. One of the most vehement opponents of the Protect America Act, Former US Representative Bob Barr (R-GA) testified in “Warrantless Surveillance and the Foreign Intelligence Surveillance Act (Part I)” (2007) about the dangers of this act. He stated that the Protect America Act allowed for the administration to secretly collect information on any American citizen “so long as the government reasonably believes one of the parties is ‘located outside of the United States.’” Barr believed this was very dangerous because of the international nature of modern communications could implicate many Americans in this

widespread dragnet. Because of this implication, Barr is particularly worried that this type of communication does not require a judicial warrant (United States House of Representatives (Part I), 2007, p.11). This lack of oversight, Barr believed, endangered privacy protections given by the Fourth Amendment for Americans who might be implicated in these searches (United States House of Representatives (Part I), 2007, p.12).

Others criticize the Act for its vagueness. Many note that the Protect America Act omits the word ‘terrorism’ or ‘terrorist’; rather it only mentions “foreign powers.” Critics believe that this omission gives the government a free license to conduct warrantless electronic surveillance on anyone engaged in any sort of international communications. Addicott and McCaul counter that the definition of a foreign power encompasses terrorism (Addicott and McCaul, 2007, p.65). The definition of a foreign power in 50 U.S.C § 1801 read:

- (1) a foreign government or any component thereof, whether or not recognized by the United States;
- (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
- (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
- (4) a group engaged in international terrorism or activities in preparation therefore;
- (5) a foreign-based political organization, not substantially composed of United States persons;
- (6) an entity that is directed and controlled by a foreign government or governments; or
- (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

According to this definition, it would seem that the potential scope of the Protect America Act would be fairly limited. It is important to note, however that the government needed only to have a reasonable belief to begin warrantless surveillance. More importantly, any Americans in any way implicated with a target can have any of their personal electronic documents monitored without a warrant; herein, lied the major controversy with the program.

Recent Developments of the Program

Despite the enormous controversy of the program for the President Bush, President Obama largely maintained the warrantless surveillance program; in fact, the Obama administration chose to expand the program. According to Nakashima (2010), “the Obama administration is seeking to make it easier for the FBI to compel companies, through National Security Letters, to turn over records of an individual's Internet activity without a court order if agents deem the information relevant to a terrorism or intelligence investigation.” The administration asked Congress to add “electronic communication transactional records” to the list of what FBI agents could obtain without a judicial warrant. The added provision would allow the FBI to collect:

the addresses to which an Internet user sends e-mail; the times and dates e-mail was sent and received; and possibly a user's browser history. It does not include, the lawyers hasten to point out, the "content" of e-mail or other Internet communication.

By allowing the FBI this information, according to former senior Bush administration Stewart A. Baker, these proposals make it easier and faster for the FBI to collect data, “and for some Internet providers, it’ll mean giving a lot more information to the FBI in response to an NSL.”

Despite campaign promises to limit the program, because of privacy concerns, Mr. Obama, continued the program where Bush left off.

This streamlining, however, worried many privacy watchdog groups. Kevin Bankstone, a staff attorney with the Electronic Frontier Foundation worried that “an expanded NSL power might be used to obtain Internet search queries and Web histories detailing every Web site visited and every file downloaded” (Nakashima, 2010). Government officials counter that electronic communication transaction records are basically email pen registers (Nakashima, 2010). Like telephone pen registers, which collect call data such a list of incoming and outgoing calls, electronic communication transaction records collect incoming and outgoing email address from a targets email account; this analogy raises interesting legal questions that will be discussed in Chapter 4.

Much of the Terrorist Surveillance Program is still classified, but the program has attracted considerable controversy for what little has been leaked. It appears that the program pushes for speed and efficiency to collect information as fast as possible in order to keep pace with communications in our fast-paced information society. The major question about this program, though, is whether its emphasis on speed and efficiency compromises Constitutionally protected civil liberties. Despite common perceptions about how far the program may intrude on our daily lives, chances are most may not really know how far the Terrorist Surveillance Program goes.

Chapter 3

“The Mechanics of the Terrorist Surveillance Program”

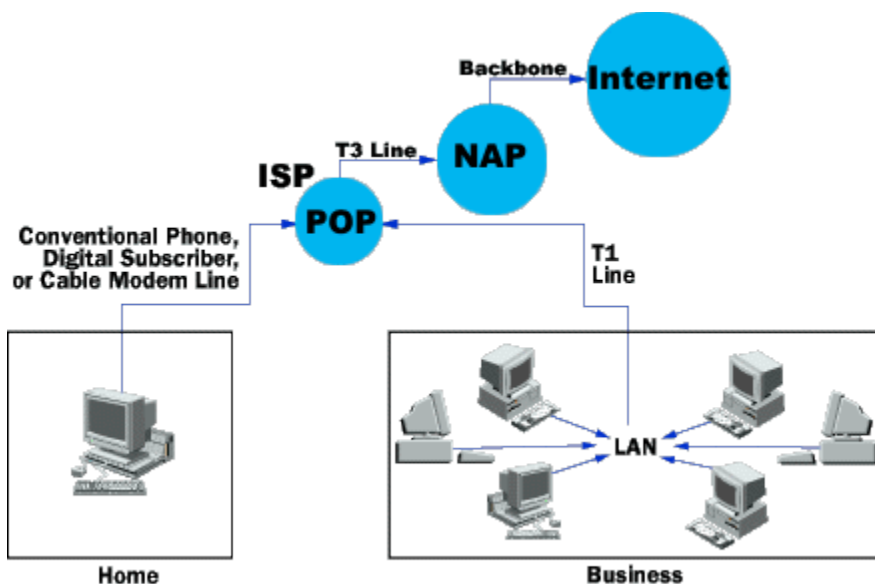
Executive power expanded dramatically under President George W. Bush. The Patriot Act granted the executive the power to unilaterally seize any personal documents from banking and telecommunication companies that might be “relevant” to a terrorist investigation. While this might be a considerable grant of power from Congress, the President—as discussed in the previous chapter—believed he had the Constitutional authority to do it anyway and much more. The Terrorist Surveillance Program, enacted shortly after 9/11, set in motion an unprecedented data mining and electronic surveillance campaign. To enact the program, the Bush administration began working with major telecommunication companies to “monitor” their customers’ data.

The Mechanics

Electronic surveillance primarily covers telephone (landlines and cellular) surveillance and Internet surveillance. While most telecommunication companies offer both services, the mediums do very different things. A telephone call in contrast to the Internet is a linear process. A call is a direct link between parties of a conversation that is directed by a telephone service provider. If the government wished to place a wiretap on one of the participants, they would just have to place a listening device somewhere either outside of the target’s call location (only if landline) or at their respective telecommunication company (for both landline and cellular phones). (Brian, 2000).

The Internet, on the other hand is a much more complicated. A personal computer must connect to a larger network through a personal T1 cable (commonly known as an Ethernet cable)

to a telecommunication company. If a group of computers are in a work or school environment, those computers are most likely on a Local Area Network (LAN) that connects to an Internet Service Provider (ISP). This smaller ISP may then merge with a larger network (Tyson, 2001, p.2) In order to meet the large amounts of data that the Internet demands, these companies set up regional a Point of Presence (POP) that bundles these access points in to one region-wide network. Then, in order to communicate between different POPs, Internet companies create agreements, called Network Access Points; these NAPs are not controlled by any one company, but rather pool the data from these separate companies into one large network that connects to the world-wide network known as the Internet (Tyson, 2001, p. 3). The figure below illustrates the structure of these networks.



(Tyson, 2001, p. 2)

In order for data to get around the Internet to a certain computer, it must first travel through a series of routers. These routers, which are specialized computers, determine where certain information goes while providing a link between separate networks. In order to determine

where this information goes, each machine connected to the Internet has a unique number called an Internet Protocol (IP) Address (Tyson, 2001, p. 4). Data that pass through these routers are called “packets.” These packets contain the IP address of the sender and the receiver, the size of the data, and the contents of the data (Diffie and Landau, 2007, p. 42). This “package” is analogous to sending a package through the mail, but for this discussion, it is also somewhat analogous to a phone call. When calling, the caller sends out information regarding where the call ought to go (a phone number) and delivers the contents (the conversation) during the call. Unlike a phone call, however, an Internet package contains both the contact information and the contents of the communication.

This difference in technology is extremely important when it comes to surveillance. For telephones, surveillance is fairly easier. For traditional landline phones, the government can install a wiretap on any part of its path to the telephone company. Digital telephone switches have made intercepting a call even easier. These wiretaps simply feed off the digital telephone switches ability to create conference calls (“A tapped call is, after all, simply a conference call with a silent and invisible third party”) (Diffie and Landau, 2007, p. 130). Phone surveillance also includes tracking logs of phone numbers. The government can track numbers in two ways. First, a pen register is a “log of the numbers of all phones called by one particular phone”; this is the list would appear on one’s phone bill. Second, a trap and trace creates a list of all the numbers that call a certain phone number (Diffie and Landau, 2007, p. 133).

The proliferation of digital phone service (known as Voice over Internet Protocol [VoIP]) and the Internet have complicated electronic surveillance. VoIP streams a phone call through an Internet network instead of a dedicated telephone line; commercial Internet phone services like Vonage operate in the same manner as the free Internet video calling service Skype. It turns out

that VoIP is inherently encrypted, which makes it much more difficult to wiretap than regular phone services (Diffie and Landau, 2007, p. 56). Being a mere part in the vast data stream of the Internet makes it even more difficult to intercept. It also is difficult, if not impossible, to separate the contact info (the equivalent of the pen register) of the Internet stream from the contents of the data package. Modern intercepting equipment “must decide in a fraction of a second whether to record a message it has detected or to permit the message to escape” (Diffie and Landau, 2007,p. 101-102). These devices sift through data and determine whether to record the data based on a number of factors including where the data is coming from, the nature of the communication, whether the information is encrypted, and where the data is going (Diffie and Landau, 2007,p. 101-102).

A pen register was given statutory protection in the Electronic Communications Privacy Act of 1986, but the Supreme Court has refused to give it Constitutional protection. According to Smith v Maryland (1979), the government may obtain a list of phone numbers because the caller has no expectation of privacy “regarding the numbers he dialed on his phone” (Smith v Maryland, 1979, p. 742). The Supreme Court believed that a list of intercepted phone numbers was not a search because the sensitive contents of the phone call itself were not revealed (Smith v Maryland, 1979, p. 741). Despite objections from Smith that the phone company handed over the pen register without his knowledge, the Court asserted that they have long held that information voluntarily given to third parties, such as the phone company, may be seized by the government without a judicial warrant (Smith v Maryland, 1979, p. 744).

Congress amended the Smith ruling by requiring a warrant to install a pen register or a trap and trace device. The process to obtain this, however, only required the government agent to merely show that the information is “relevant to an ongoing investigation” (Slobogin, 2007, p.

171). The Patriot Act expanded this process to any electronic communication. It is important to note that if the government agent shows that the information is relevant to an ongoing investigation, the judge *must* grant the warrant (p.172). The easy process to obtain a warrant appeased the government's demand for a more efficient way to obtain government surveillance, but the government wanted more than simple access to communications.

Government Data Mining Before 9/11: Carnivore

News leaks about a previous intercepting system gives clues about modern intercepting systems associated with the Terrorist Surveillance Program. One of these systems, Carnivore, was probably the most notorious interception program and served as a precursor to the modern Terrorist Surveillance Program. Carnivore, began as an FBI program in 1997 to collect online information such as email and bank histories (Konrad, 2000). The FBI approached several Internet Service Providers in the late 1990s about installing Carnivore into their systems to ease electronic surveillance efforts (O'Harrow 2005, p.257). Diffie and Landau (2007), give a detailed overview of the program:

Carnivore was a *packet sniffer*, a program that analyzes network traffic; such a program can be configured to search for traffic to or from a particular user. ISPs serve as the local post offices of the Internet world, sorting and delivering email and other services to other users. When Carnivore was placed at an ISP, it received all packets that traversed the Ethernet connection on which it was placed . . . Using filters, Carnivore recorded the traffic that fit pre-determined patterns, generally traffic to or from a particular user. Carnivore could be configured for full wiretap or pen register mode (p. 269)

The FBI assured these ISPs they would have to get a court order before they implemented it for investigations. They mentioned nothing at the time, however, about data mining for non-criminal investigations (O' Harrow 2005, p. 257).

Not all ISPs willingly worked with the FBI, however. A number of companies refused to install Carnivore. EarthLink, one of the nation's largest ISPs at the time objected because it "slowed the company's computers and took more information about consumers than it was legally entitled to" (O' Harrow 2005, p. 257). The company sued the government to stop the program, but it lost the case. However, the company came to an agreement with the government that if it conducted its own surveillance and reported its findings to the government, it would not have to install Carnivore (O' Harrow 2005, p. 257). On July 11, 2000, the Wall Street Journal leaked information about the FBI's use of Carnivore, by then called DCS 1000 (Diffie and Landau 2007, p. 269). The program caused an uproar in Congress, according to Konrad 2005, especially with Senators Orrin Hatch (R-Utah) and Patrick Leahy (D-Vermont), the respective Chairman and Ranking Member of the Senate Judiciary Committee. In September 2000, the House Judiciary Committee voted 20-1 to restrict the FBI's use of Carnivore. Due to the controversy, and outdated technology, the FBI discarded DCS 1000 around 2003 (Slobogin 2007, p.11).

Government Data Mining After 9/11

The FBI ditched Carnivore because it no longer needed it. By 2003, a plethora of private data mining firms had emerged with most of the data the government had been seeking. The use of private data brokers, however, signaled the government's intentions of going beyond mere wiretapping. The government sought to amass the online information of the American people in

a government database. The Terrorist Surveillance Program used data from companies such as ChoicePoint and Lexis-Nexis to collect vast amounts of computerized personal data (O' Harrow 2005, p. 250). Programs like ChoicePoint and LexisNexis compiled vast amounts of personal data from credit reports that include: name address, previous address, phone number, social security number, . . . employer . . . financial reports, education records . . . information about family members" (Slobogin, 2007, p. 10). ChoicePoint and LexisNexis could purchase these records easily without fear of legal repercussions. Privacy laws that prevented the government from obtaining the same information did not apply to private corporations (Slobogin, 2007, p. 11). These companies could hand over information to other companies who were willing to purchase it and to the government for a similar fee without a government warrant because it was third party information (Young, 2007).

The idea for a massive government database began in 1999. John Poindexter presented the idea of this database, called "Total Information Awareness," to his colleagues at the Defense Advanced Research Projects Agency (DARPA) in January. At first, his colleagues did not give the project too much thought (O'Harrow, 2005, p. 190-191). After the 9/11 attacks, however, the Justice Department became very interested in Mr. Poindexter's vision and decided to begin data mining shortly thereafter (O'Harrow, 2005, p. 290). The overall goal of "Total Information Awareness" was to "use gargantuan database technologies to scan billions of bits of transactional data to weed out possible terrorist patterns." The program was to interpret Internet search queries to determine terrorist plots (Young, 2007). A former NSA data analyst David Holtzman said "to really do this right, you have to put everybody into the net." Ultimately, Total Information Awareness would include the personal data of millions of American citizens (banking records, spending habits, and family and educational backgrounds) into one massive

database; all of this would be conducted without telling the American people. *New York Times* columnist William Safire, however, wrote about the controversial program on November 14, 2002, about one year after the start of the program; the article was titled “You Are a Suspect” (O’ Harrow 2005, p. 204). Safire’s scathing article proclaimed:

If the Homeland Security Act is not amended before passage, here is what will happen to you: Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend -- all these transactions and communications will go into what the Defense Department describes as "a virtual, centralized grand database" (Safire, 2002, p. 1).

The article triggered calls in Congress to end the program; Congress succeeded in ending funding for Total Information Awareness the following February (O’ Harrow 2005, p. 205-206).

But how did “Total Information Awareness” work? When the FBI ditched Carnivore, it began using private data brokers (Diffie and Landau 2007, p. 271). In fact, most of Total Information Awareness depended on these data brokers. In fact, the government preferred using private data brokers. According to Slobogin (2007), “under current law, law enforcement officials do not need even a certification order to use ChoicePoint or similar computerized vehicles for public documents,” nor do they need to consult any other government entity (p. 172). This process required less legal hurdles compared to traditional search methods. As mentioned earlier, the Supreme Court did not give Constitutional protections to information voluntarily given to third parties (p. 172). While the Privacy Act of 1972 did limit personal access to such data, government officials merely needed permission from head of their respective

department stating that the information is relevant to an ongoing investigation (p. 173). Initially, Watergate-era reforms restricted this process, but after 9/11, President Bush “lifted the restraints and pushed agencies aggressively to use private databases; an internal FBI document, for example, stated “Use ChoicePoint to your heart’s content” (Young 2007).

However, private data brokers were only a part of Total Information Awareness. At the beginning of Total Information Awareness, the FBI planned to build a “centralized information system . . . that would combine criminal, intelligence, and commercial records” (O’ Harrow, 2005, p. 208). This, evidently, is one program among many. Slobogin (2007) estimated “the federal government alone probably operates more than 200 data-mining programs, at least which involve efforts to obtain personal information such as credit reports and credit card transaction records” (Slobogin, 2007, p. 192). Programs like Threat and Local Observation Notice (TALON) collected “information on thousands of American citizens who protested the war in Iraq and other government policies and then made the data accessible to 28 government organization and more than 3,500 government officials. Another program, Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE) was designed “to troll a vast sea of information, including audio and visual, and extract suspicious people, places and other elements based on their links and behavioral programs” (Slobogin, 2007, p. 169).

The government’s surveillance programs expanded beyond Total Information Awareness. The overall purpose of government surveillance was to stop terrorist plots and to apprehend those who plan them. In order to do this effectively, the government had to rely on first hand information. One of the more startling ways the government accomplished this was through directly filtering information going through telecommunication companies. As mentioned in the previous chapter, Mark Klein stumbled upon the secret NSA “splitter room.” The room copied

the data stream of AT&T San Francisco branch's customers and sent it to a super computer for further analysis. This data was sent to the secret NSA room, a room that only NSA approved individuals could enter, that connected to a Narsus STA 6400. This system evidently operated like the then-defunct Carnivore. Steve Bannerman, Vice President of Narsus Marketing told Frontline about the mechanics of the system:

It's sort of analogous to a letter inside of an envelope. So you've got different layers in these things we call packets. And you know, the first layer that you get to peer back is the information about where the packet's coming from and where it's going to, the addresses that identify, you know, who's communicating with who. And then once you've delved into deeper parts of the packets, that's when you get into what's called the payload, and that includes the actual information that you're trying to send in the packet (Young, 2007).

Like Carnivore, Narsus, a privately developed program that, "sniffed" packets by certain search criteria and sent those packets to the NSA for further analysis. Scott Marcus, a former Federal Communications Commission expert "estimated that they set up eavesdropping rooms at 15 to 20 sites across the U.S., intercepting about "10 percent of all purely domestic" Internet traffic. And that's just at AT&T" (Young, 2007). While ten percent may seem small, the disturbing concept behind Narsus focuses on *how* it collected information. In order to filter information, Narsus searched through both the identifying information *and* the contents of Internet data without any judicial oversight. This would be analogous to having the post office open every bit of mail and sorting it based on what the actual letter said; a practice outlawed both by statute and the Constitution.

The overall goal of this massive data collection campaign was to assemble the world's largest database of phone calls and Internet data. One of the purposes of the database was to “analyze calling patterns in an effort to detect terrorist activity” (Cauley, 2006). The Bush Administration commented that the program merely eavesdrops—without warrants—“on international calls and international e-mails of people suspected of having links to terrorists when one party to the communication is in the USA” (Cauley, 2006). Sources, however, say that the program goes much deeper. The database reportedly had:

access to records of billions of domestic calls, the NSA has gained a secret window into the communications habits of millions of Americans. Customers' names, street addresses and other personal information are not being handed over as part of NSA's domestic program, the sources said. But the phone numbers the NSA collects can easily be cross-checked with other databases to obtain that information (Slobogin 2007, p. 194).

The NSA contended that the database needs to contain this vast amount of calling data in order to sniff out terrorist plots. Ultimately, the NSA is trying to:

whittle down the hundreds of millions of phone numbers harvested to hundreds of thousands that fit certain profiles it finds interesting; those in turn are cross-checked with other intelligence databases to find, perhaps, a few thousand that warrant more investigation (Slobogin 2007, p. 194).

The vast reach of the program may have irked many Americans, but the NSA—and the Bush Administration as a whole—seemed willing to use the best tactics to prevent another terrorist attack.

The Cooperation of Telecommunication Companies

In order to wage the War on Terror effectively, the Bush administration recruited the help of telecommunication companies. The NSA, however, did not simply invade AT&T and install the Narsus computers against their will. In his suit against the government, Mark Klein, the former employee who first discovered the computers, alleged that AT&T unlawfully allowed the government to copy their customer's live data; AT&T and the NSA refused comment, but urged that the case be dismissed citing state secrets. Klein eventually lost the case because he could not prove he was personally spied on by the program (Young, 2007). Other lawsuits followed. On May 12, 2006, attorneys Bruce Afran and Carl Mayer filed suit against Verizon claiming that, like AT&T, Verizon unlawfully turned customers' information to the NSA. The lawsuit claimed that the company violated the Communications Act of 1934, the Electronic Communications and Privacy Act, and the Stored Communications Act of 1986. While the suit claimed that Verizon unlawfully handed over phone records, it did not mention whether Internet data was also handed over; it is possible, however, that Afran and Mayer omitted Internet data from the suit because it appeared that the NSA had full legal authority to collect said data. AT&T was involved in a similar suit. The government asked the case be dismissed on national security grounds (Reardon, 2006).

Understandably, many were concerned about the interception of live data; but retained data may be the bigger threat to civil liberties. As mentioned earlier, the government sought to amass a databank of recorded calls. While live interception enraged members of Congress, many supported, and even pushed for, telecommunication companies to retain customer data and hand it over without a judicial warrant for reason other than terrorism prevention. Between 2005 and 2007, the Justice Department and members of Congress pushed for a bill that would require ISPs

to retain records of their customers' data. Initially, Congress petitioned data retention to prevent the spread of child pornography and the apprehension of offenders. In 2005, however, the Justice Department petitioned Congress to mandate telecommunication companies to maintain records of "email chatter, Web browsing or chat-room activity" for a specific amount of time to help with the Terrorist Surveillance Program. It appeared that the Justice Department wanted to improve upon the Electronic Communication Transactional Records Act of 1996, which required "Internet providers to retain any 'record' in their possession for 90 days 'upon the request of a governmental entity.'" This original bill, however, only required data preservation rather than data prevention. At the time:

Internet service providers typically discard[ed] any log file[s] that's no longer required for business reasons such as network monitoring, fraud prevention or billing disputes.

Companies [did], however, alter that general rule when contacted by police performing an investigation (McCullagh, 2005, p.1).

In addition, ISPs were required to report sightings of child pornography to the National Center for Missing and Exploited Children, "which is in turn charged with forwarding that report to the appropriate police agency" (Broache and McCullagh 2006a). The traditional policy, data preservation, only began when the government (with a warrant) ordered the company to begin recording an *individual's* data. On the other hand, data retention would mandate that *all* data on *all* customers would need to be retained for a certain period of time without a warrant. Such a widespread collection of data is unprecedented in United States history.

Nonetheless, the Justice Department and some members of Congress believed such a large collection of data was necessary for the information age. The proposed laws would do more than prevent terrorist plots. Representative Diana DeGette (D-Colorado), stated during a May

2006 hearing that data retention “laws were necessary to thwart child pornographers and other Internet predators” (Broache and McCullagh 2006a). A few weeks later, Attorney General Alberto Gonzales, in a private meeting with telecommunication industry representatives, echoed Rep. DeGette’s calls for data retention to help with prosecutions of child pornography. He argued that Internet companies often automatically deleted data unless they had a specific use. Gonzales’s proposal would allow government agents to stop the exploitation of children in a more timely and efficient matter. Gonzales pushed the issue further in a September 2006 Senate Banking Committee hearing: “We need to figure out a way to have ISPs retain data for a sufficient period of time that would allow us to go back and retrieve it” (Broache and McCullagh, 2006b). The Republicans on the committee, led by Sen. John McCain, agreed with Gonzales. Among the proposed amendments to the bill, one would require “Internet providers and perhaps social-networking sites and search engines to record for a year or two which IP address is used by which user” (Broache and McCullagh, 2006b). Another proposed amendment went further requiring “companies to record data such as the identities of e-mail correspondents, logs of who sent and received instant messages (but not the content of those communications), and the addresses of Web pages visited” (Broache and McCullagh, 2006b). Critics point out, however, that the retained data would not be limited to child pornography cases, nor would there be limits placed on what files the FBI could pull from the retained records (Broache and McCullagh, 2006b).

Despite its controversial nature, the FBI nonetheless continued to push the bill. In July 2006, the FBI stated that their draft of a data retention bill would be introduced by Sen. Mike DeWine (R-Ohio). The FBI stated that the bill, would help “thwart criminals and terrorists who

have turned to technologies like voice over Internet Protocol, or VoIP” (Broache and McCullagh, 2006b). The FBI further stated the necessity of the bill:

The complexity and variety of communications technologies have dramatically increased in recent years, and the lawful intercept capabilities of the federal, state and local law enforcement community have been under continual stress, and in many cases have decreased or become impossible (Broache and McCullagh, 2006b).

As mentioned earlier, with the advent of VoIP, phone surveillance had become tangled in Internet surveillance; thus it was difficult to apply phone surveillance law. Some of the most noteworthy amendments of the proposed data retention bill would:

- Require any manufacturer of "routing" and "addressing" hardware to offer upgrades or other "modifications" that are needed to support Internet wiretapping.
- Authorize the expansion of wiretapping requirements to "commercial" Internet services including instant messaging [a service similar to text messaging, but between two Internet users rather than two cell phone users] if the FCC deems it to be in the "public interest." That would likely sweep in services such as in-game chats offered by Microsoft's Xbox 360 gaming system as well.
- Force Internet service providers to sift through their customers' communications to identify, for instance, only VoIP calls. (The language requires companies to adhere to "processing or filtering methods or procedures applied by a law enforcement agency.") That means police could simply ask broadband providers like AT&T, Comcast or Verizon for wiretap info--instead of having to figure out what VoIP service was being used.

- Eliminate the current legal requirement saying the Justice Department must publish a public "notice of the actual number of communications interceptions" every year. That notice currently also must disclose the "maximum capacity" required to accommodate all of the legally authorized taps that government agencies will "conduct and use simultaneously" (Broache and McCullagh, 2006b).

Not surprisingly, the bill garnered a lot of controversy. Despite the FBI's backing, the bill was never introduced because Republicans wanted to avoid controversy in an election year. Although the bill was never formally introduced, the draft of the bill gives the public an insight into Congression intentions. According to, in February 2007, Representative Lamar Smith (R-Texas), reintroduced data retention as a part of the Safety Act. The bill remained similar to the previous data retention bill (McCullagh, 2007, p.1). McCullagh noted that this bill placed no limit "on how broad the rules can be, Gonzales would be permitted to force Internet providers to keep logs of Web browsing, instant message exchanges, or e-mail conversations indefinitely" (p.2). As of today, Congress has not passed the Safety Act.

The FBI's aggressive push for mandatory data retention has been a relatively quiet issue compared to the interception of live data; but the FBI seems to place more emphasis on the former rather than the latter. Slobogin (2007) explained that legally, it is much easier:

Under [the Electronic Communication Privacy Act], real time interception of the content of phone and e-mail communications requires a warrant based on probable cause. But if e-mail has sat on a server for longer than 180 days without being opened *or* the recipient of e-mail or voice mail accesses it and stores it on an outside server for any length of time, then a subpoena—delayed if necessary [i.e. could acquire information in an

emergency situation, then apply for a retroactive subpoena]—is all that is needed to obtain the content of the communication (p. 175).

Thus, if telecommunication companies were required to retain *all* of their customers' data, there would seemingly be no need to use live intercepting equipment for a database. In other words, it appeared that the FBI may have planned to use retained data to operate a "Total Information Awareness"-like database to sniff out terrorist plots, while using the Narsus computers to intercept data on targets selected through other means including the aforementioned vast database. In this sense, the Terrorist Surveillance Program has grown to almost Orwellian heights of governmental surveillance; turns out it does not stop at mere communication surveillance.

National Security Letters

The other part of the Terrorist Surveillance Program, National Security Letters, added another dimension to the Terrorist Surveillance Program., National Security Letters came from a provision in Electronic Communications Privacy Act as an efficient means to collect customer information from financial corporations. Congress created the bill after a Supreme Court ruling that refused to grant Fourth Amendment protection to information voluntarily given to third parties. Originally, ECPA limited the use of NSLs to information "relevant to an authorized foreign counter-intelligence investigation" (Garlinger, 2009, p.1110). In order to obtain an NSL a government agent must have "specific and articulable [sic] facts" showing a nexus between the information sought and "a foreign power or an agent of a foreign power"(Garlinger, 2009, p.1110). The NSL was very useful because it allowed a speedy seizure of financial information; the Bush administration viewed this as an effective tool.

The Patriot Act, in Section 505 dramatically expanded the use of Nation Security Letters in a few ways. First, it allowed NSLs “to protect against international terrorism or clandestine intelligence activities” instead of only pure foreign investigations (Garlinger, 2009, p. 1111). This change preserved the original exception in FISA that allowed the President sole discretion in purely foreign intelligence matters. Second, it relaxed the standard from requiring "specific and articulable facts" to show that the information is related to the target, to merely showing that said information would be relevant (Garlinger, 2009, p. 1111). Third, the act expanded the information that an NSL could obtain. It expanded from “financial data, telephone records, and consumer credit reports” to information such as “types of services used any ‘temporary assigned network addresses,’ and sources of payment” (Garlinger, 2009, p. 1111).

In the Information Age, the implications of the expanded use of the National Security Letter prove to be quite invasive. For example, Frontline interviewed Alan Feldman, Senior Vice President of the MGM Mirage in Las Vegas. In December 2003, Feldman stated that FBI agents demanded that the casino hand over “all of [its] records;” “all of the records” at the hotel included: “The hotel records, the airline records, the rental car records, the gift shop records, the casino records” (Young, 2007). Frontline reported that several other casinos were approached with the same request. Indeed O’Harrow (2005) confirmed that the FBI conducted a major “information sweep” in cities threatened by a terrorist attack across the country. During this information raid, the FBI gathered information such as “names, addresses, credit card numbers . . . passenger manifests” driver’s license information from car rental agencies and storage facilities (O’ Harrow, 2005, p. 248). The FBI evidently looked for certain patterns in these records that resembled terrorist activity. By Christmas Eve, the FBI collected “hundreds of thousands of business records” (O’ Harrow, 2005, p. 249). It should not be surprising that the much of

society's personal information is trusted to third parties, given the modern push to digitize information. Many might be surprised, however, that the same information is able to be seized by the FBI without a warrant.

The information obtained by the FBI is sensitive information on millions of Americans and tourists. These massive secret data sweeps that collected personal financial information were conducted without any specific foreign target; the FBI, however, can obtain this information with ease. As mentioned earlier, since the information given to third parties is not given Fourth Amendment protection when it is seized by the government, it therefore does not require a judicial warrant. To avoid controversy, Congress set up loose measures to give minimal protection to this increasingly vital information; of course, the Patriot Act relaxed these standards further. A National Security Letter only required certification from a special agent (a field agent) that "the information sought is relevant to an investigation designed to protect against international terrorism or clandestine intelligence activities" (Slobogin 2007, p. 177). The subpoena process given no judicial review. In fact, recipients were barred from seeking judicial review (Garlinger 2009, p. 1125). Furthermore, the recipients were gagged from disclosing to anyone who would not be needed to hand over the materials in question (Slobogin 2007, p. 177). Clearly, the FBI's had an (alarmingly) easy process to obtain a NSL.

The ease of obtaining an NSL is one reason why its use became very popular. "The FBI alone issues roughly 30,000 to 50,000 NSLs a year and maintains all the records obtained (even when they are not linked to terrorism)" (Slobogin, 2007, p. 179). This widespread use of these permissive subpoenas spurned many lawsuits. In 2004, a federal district court judge ruled the entire NSL authorization scheme unconstitutional; another court agreed in 2005. Mounting legal challenges and Congressional worries led to amendments to the Patriot Act that would, among

other things, allow third parties to challenge an NSL when they are “unreasonable, oppressive, or otherwise unlawful” and to challenge the accompanying gag order as well. Congress did nothing to limit the actual process of obtaining an NSL nor did it limit the scope of what it could legally seize.

The scope of the Terrorist Surveillance Program is eye-opening. The prospect of a massive database containing American’s spending habits, Internet activities, financial information, phone calls, and other personal information sounds like it belongs in a dystopian novel. To put the program in tangible terms, imagine an FBI official pulling up your Internet search queries from this database at any time they wish without your knowledge; this is a very real possibility under the current program. Perhaps even more disturbing is that the initial stages of the program do not target anybody; they target *everybody*. The government’s emphasis on terrorist *prevention* has replaced the traditional purpose of surveillance: to catch crime rather than prevent it. While it may be effective, the big question looming over the Terrorist Surveillance Program is whether it is actually legal.

Chapter 4

“The Constitutionality of the Terrorist Surveillance Program”

Before the age of the computer, it was impossible to conduct a nation-wide monitoring of one's activities. Many personal documents—financial records, personal letters, and personal purchases—thirty years ago could be simply torn, burned, or thrown away if the owner did not want anyone else to view them. Today is a different story. Much of our lives live on the Internet. While this may be a convenience, the Information Age certainly has its drawbacks. It is now easier for the government to intrude on our daily lives. The ultimate goal of the Terrorist Surveillance Program is to have a quick and effective system to root out and stop terrorist plots. In order to do this, however, the government wishes to data mine the personal information of millions of Americans. While it may turn out to be an effective tool for the War on Terror, the question for the Terrorist Surveillance Program faces two important Constitutional questions: Whether it violated the Fourth Amendment as an intrusive and unreasonable search; and whether President Bush had the Constitutional authority to unilaterally authorize the program.

The Doe Cases

A 2004 case questioned whether the Terrorist Surveillance Program could pass Constitutional muster. Doe v. Ashcroft (2004) ruled that the FBI's use and enforcement of National Security Letters (NSLs) violated the First and Fourth Amendments to the Constitution as well as several privacy laws. The plaintiffs, an unnamed Internet Service Provider under the pseudonym “John Doe” who were represented by the American Civil Liberties Union and the American Civil Liberties Union Foundation, contested a National Security Letter issued to them

by the FBI (Doe v. Ashcroft, 2004, pgs. 474-475). The District Judge, Victor Marrero, however, noted that the NSL can obtain “basic subscriber [information]” which included:

(1) a subscriber’s name and (2) address; (3) the subscriber’s local distance telephone connection records, or records of session times and durations; (4) the subscriber’s length of service and types of service he has utilized; (5) any telephone or instrument [including an Internet Protocol (your unique Internet “phone number”)] or other subscriber number or identity, including any temporarily assigned network address; and (6) the subscriber’s means and source of payment for the service (p. 487).

This subscriber information is similar to a pen register in that they both detail information of the communication, but not the contents of that communication. Despite the similarity, the legal way to obtain Internet subscriber information is much different from obtaining a pen register (Doe v. Ashcroft, 2004, p. 489). The Supreme Court refused to give Fourth Amendment Protection to pen registers in Smith v. Maryland (1979) because there is no expectation of privacy [the Constitutional standard set in Katz] in a list of phone numbers given to a phone company. Congress, however, stated in the Electronic Communications Privacy Act (ECPA) that the government obtain a warrant before such a search in order to get a pen register (Doe v. Ashcroft, 2004, p. 481). The NSL, on the other hand, obtained Internet subscriber information without judicial approval. While pen registers and Internet subscriber information may be similar, Judge Marrero ruled that the NSL did not violate the ECPA. Rather, the FBI correctly applied the NSL in congruence with its prescribed use in the Patriot Act.

The NSL provision in the Patriot act, itself, however violated the ISPs Fourth Amendment rights. Judge Marrero (2004) ruled that the law as written is an unreasonable search of the property of the Internet Service Provider (Doe v. Ashcroft, 2004, p. 494). The NSL

process provided no judicial oversight to confirm whether the search was reasonable.

Administrative subpoenas, like a NSL, merely required a “reasonable” belief that a suspect is committing a crime. The problem with the NSL, however, was that it obtained personal information from corporations *without* any sort of judicial oversight. Even though the law mandated the relaxed “reasonableness” standard before it was executed, it did not demand that this judgment come from an independent magistrate. Marrero (2004) pointed out that “the Supreme Court [in See v. Seattle (1967)] held that an administrative subpoena ‘may not be made and enforced’ by the administrative agency” (Doe v. Ashcroft, 2004, p. 435). The law also violated the Fourth Amendment because it bared the recipient from challenging a National Security Letter. Marrero (2004) wrote “access to legal advice and availability of judicial process to enforce and contest the law” is vital to the protections of the Fourth Amendment (Doe v. Ashcroft, 2004, p. 501). Ultimately, the NSLs lack of judicial oversight proved to be its downfall rather than the information it sought.

Fourth Amendment protection is not, however, given to subscribers. Marrero (2004) noted the Fourth Amendment cannot be applied for subscriber’s information because they had voluntarily submitted it to a third party. The Supreme Court ruled in United States v. Miller (1976) that information voluntarily given to a third party (like a bank) does not have a reasonable expectation of privacy and therefore is not given protected by the Fourth Amendment (Doe v. Ashcroft, 2004, p. 494). Given that the subscriber’s information is clearly not given protection by the Fourth Amendment from an unwarranted search, Marrero (2004) seemingly had no argument to strike down the law in regards to subscribers. Nonetheless, he believed that the law might actually violate the subscriber’s First Amendment right to freedom of association. This right, recognized by the Supreme Court in NAACP v. Alabama (1958), prevented both the state or

federal government from compelling an organization to divulge a list of membership. Marrero (2004) related the NAACP case with the Doe case: “‘compelled disclosure, of affiliation with groups engaged in advocacy’ amounts to a ‘restraint on freedom of association’ where disclosure could expose the members to ‘public hostility’” (Doe v. Ashcroft, 2004, p. 507 [qtd. from NAACP v. Alabama (1958, 357 U.S. 462)]).

Garlinger (2009), however, found fault with this First Amendment privacy logic. He noted that the First Amendment¹ protects the “liberty to interact with others through speech without fear of government suppression or reproach” (p. 1128). Marrero (2004), on the other hand, used the First Amendment to protect customers from unwarranted government intrusion and the subscriber’s “freedom of anonymous Internet search” (Doe v Ashcroft (2004), p. 508). Garlinger, however, contended that emails are not anonymous speech because both the recipient and the sender are indicated in an email. It seemed that the First Amendment argument is a stretch when it comes to Internet surveillance. Marrero’s (2004) logic seemed to apply to anonymous Internet forums, but cannot be easily applied to other Internet activity such as emailing and browsing histories. The First Amendment controversy did not matter, however, in the appeal because the case was rendered moot with the USA PATRIOT Improvement and Reauthorization Act of 2005, which added provisions that would allow the recipient to contest an NSL in court. However, the administrative authorization process remained intact (Doe v. Gonzales (2005), p. 4).

¹ For text of the First Amendment, see Appendix 1

It Does Not Belong to You

Judge Marrero had to jump through legal hoops to argue that a government search of a customer's private Internet habits was intrusive, but why? Is what we do and what we have on the Internet really our property? According to the Supreme Court, it is not.

It begins with a case involving the banking records. In United States v. Miller (1976), the Bureau of Alcohol, Tobacco, and Firearms subpoenaed Mr. Miller's bank for his financial records (United States v. Miller, 1976, p. 437). Miller contended the subpoena was an unreasonable search of his private papers. The Court, however, ruled that Mr. Miller's banking records were not his; rather, they were business records of the bank. Even if the records, the Court reasoned, did belong to Miller, he had no reasonable expectation of privacy because he willingly gave the papers to a third party (United States v. Miller, 1976, p.442). The Court extended this third party doctrine to telephone pen registers in Smith v. Maryland (1979). Thirty years later, other courts applied Miller and Smith to the Internet in US v. Kennedy (2000) and Guest v. Leis (2001).

In United States v. Kennedy (2000), the Internet Service Provider, Road Runner, informed state officials of a subscriber who had downloaded child pornography. From that point, the FBI began an investigation, which ultimately led to Mr. Kennedy's arrest (United States v. Kennedy, 2000, p.1106). Kennedy moved to remove the evidence obtained from the ISP because he believed the FBI violated both the Electronic Communications Privacy Act and the Fourth Amendment by not first seeking a warrant (United States v. Kennedy, 2000, p. 1108). While the United States District Court of Kansas agreed that the government did violate the ECPA—which stated that a provider of electronic communication can only give subscriber information when presented with a court order—it did not believe that the FBI violated the Fourth Amendment

(United States v. Kennedy, 2000, p.1109-1110). Like the Miller ruling, the court agreed that any information voluntarily given to a third party loses all legitimate expectations of privacy and therefore did not require a warrant to obtain Mr. Miller's records (United States v. Kennedy, 2000, p. 1110).

Similarly, in Guest v. Leis (2001), a local sheriff's department searched an online bulletin board for obscene files. The sheriff stated that he found forty-five obscene images on the board and from there obtained a warrant to examine the computers of the offenders. In the search, the Plaintiffs (Guest et al.) contended that the sheriff's department looked through their emails; the sheriff's department contended it did not (Guest v. Leis, 2001, p. 331). The Plaintiffs argued that the sheriff department violated their Fourth Amendment rights in the illegal search. The Court of Appeals for the Sixth Circuit, however, ruled that the Fourth Amendment had nothing to do with the search. The Court stated that there is no reasonable expectation of privacy in posting on a public bulletin board nor are there protections for an email that had reached its recipient (Guest v. Leis, 2001, p. 333). That is to say, according to the Guest court any email that is sent automatically loses any Fourth Amendment protection as well as anything posted onto a public Internet forum.

The courts in both Kennedy and Guest treated the Internet as a simple business transaction between a subscriber and the ISP. Many scholars took issue with this third party doctrine created in Miller. Slobogin² (2007), for one, believed that the Miller ruling was very unrealistic in the modern world. He wrote:

“the first problem [with Miller] . . . is that the Court simply defies reality when it says that one voluntarily surrenders information to doctor, banks, schools, and phone and

² Christopher Slobogin is a professor at the Vanderbilt University of Law. He is one the most notable authors on modern surveillance law.

Internet providers. It is impossible to get treatment, engage in financial transactions, obtain an education, or communicate with others without providing personal information to the relevant facilitating entities or allowing those entities to collect it. To choose to forgo these activities would mean an isolated, unproductive, and possibly foreshortened existence (p.156).

Slobogin raised an interesting point. In today's society, it is extremely difficult to function in everyday society without some form of technology. Even menial tasks like visiting the doctor require that a patient give sensitive information. Another seemingly menial task, shopping for groceries might entail using a credit card that is instantly stored on the company's computers. The pervasiveness of electronic record-keeping might make modern living a convenience, but it can also track what we do to uncomfortable extent.

According to Miller, the record of commercial transactions belongs to the respective companies. To put it another way, anything that a customer does on the Internet is, legally, a copy of business records of the ISP rather than the browsing history of the individual user. Slobogin (2007) took issue with this logic. He wrote, "although the physical documents maintained by third party record holders may be the third party's property alone, their content generally is not wholly within their control" (p. 157). Some argue, however, that customers still choose to give personal information to third parties and therefore must assume the risk that those companies could disseminate that information for its business transactions. Slobogin argued, however, people must give information to companies if they are to properly function in modern society (p. 158). It is true that in some instances it is absolutely necessary to give personal information to a third party. For example, if involved you are in an accident, you must give basic and medical information in order to receive medical care. In order to attend a school (both

compulsory schooling and higher education), a parent and/or student must surrender personal information if they are to attend that school. While emails and phone calls may not be absolutely necessary to function, it is becoming increasingly difficult to function without them.

For this reason, it appeared that the courts slowly have limited the third party doctrine. Slobogin (2008) noted that several recent cases have removed the Miller precedent in a few key areas. For example, in Ferguson v. City of Charleston (2001) the Supreme Court ruled that a hospital automatically turning over the results of pregnancy tests to the police without the women's consent was a violation of the Fourth Amendment (Slobogin, 2008, p. 330). While this may be an extreme case, the Supreme Court seemed to whittle down the basic principle that individuals who give information to third parties surrender control of that information. Furthermore, lower courts have further eroded the reach of Miller. Slobogin (2008) noted a case law survey from Stephen Henderson, published in the Pepperdine Law Review, that summarized what lower courts have considered when not applying Miller to cases involving third parties:

(1) the extent to which disclosure of the information is necessary to function in society (with one court, for instance, distinguishing between phone numbers maintained by the phone company and information given to a locksmith³); (2) the degree to which the information is personal (with one court, for example, evidencing deep disagreement over whether [electric] power consumption records are personal⁴); and (3) the amount of information obtained (with some courts distinguishing between multiple records and a record of one transaction⁵) (Slobogin, 2008, p. 331).

³ People v. Abbot 208 Cal Rptr 738, 741 (1984).

⁴ In re Maxfield 945 P2d 196 (Wash 1997).

⁵ Commonwealth v. Duncan 817 A2d 455, 463 (Pa 2003).

The Curious Case of Pen Registers

The third party doctrine does not automatically eliminate Internet communications from Fourth Amendment protection. The legality of pen registers provides an interesting argument to protect Internet communications. In Smith v. Maryland (1979), the Supreme Court determined that there is no “reasonable expectation of privacy” with the list of phone numbers one calls. In the case, the government installed a pen register, which accumulated a list of phone numbers that Mr. Smith dialed (Smith v. Maryland, 1979, p. 737). The pen register was installed within the telephone company; therefore, the device itself did not invade Mr. Smith’s property (Smith v. Maryland, 1979, p. 741). Nonetheless, Mr. Smith argued that Katz v. United States (1967) (which ruled that a warrant was necessary for wiretap on a public phone) granted him Constitutional protection from unwarranted government intrusion (Smith v. Maryland, 1979, p. 739). The Court, however, makes a distinction between the wiretap (as in Katz) and the pen register in the present case. Justice Blackmun cited a previous case (United States v. New York Tel. Co. (1977)) to explain pen registers:

“Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed – a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, not whether the call even complete is disclosed [sic] by pen registers” (Smith v. Maryland, 1979, p. 741).

Unlike the wiretap in Katz, the government did not capture the contents of the call, but rather the list of phone numbers Mr. Smith dialed. The court reasoned he had to realize the phone company would know the phone numbers he dialed in order to complete the routing and for billing

purposes (Smith v. Maryland, 1979, p. 742). A number of lower courts have adapted the Smith ruling to ISP in number of cases including United States v. Kennedy and Thygeson v. U.S. Bancroft (2004) with the same rationale that ISP subscribers knowingly gave routing information to the company in order to complete the transaction (Slobogin, 2007, p. 171). However, Congress has given minimal protection for this type of surveillance. Congress approved a streamlined subpoena process for pen registers in the Electronic Communications Privacy Act of 1986 and with Internet surveillance in the Patriot Act of 2001. This process merely required the government to show that information sought was “relevant to an ongoing investigation” and that the information is “likely to be obtained by [the surveillance]” (Slobogin, 2007, p. 171).

While given the same legal protections, Internet logs divulge much more than a pen register. As mentioned earlier, Internet communication is fundamentally different from telephone communication. Ditzion (2004) notes the flaw in the analogy of pen registers with Internet surveillance:

The reasoning of Smith v. Maryland simply does not apply to the Internet. Smith relied on the fact that telephone users disclosed discrete signaling information to third parties, and this information could easily be intercepted using technology that would not also reveal the content of conversations [. . .] the Smith majority was at least able to draw an easy-to-implement and technically practical line. On the Internet, there is no longer such a clear line to draw. Users disclose both content and routing information, in exactly the same technical manner, to an enormous number of third parties. The exact same computer read both content and routing information, which are frequently intermingled within packets. The only way that Smith’s reasoning based on third-party disclosure could make sense in the Internet age would be an undesirable (and likely factually

inaccurate) holding that people have no expectation of any privacy in their Internet communication (p. 1336).

It is also important to note that the act of accessing a web site is radically different from making a phone call. When the government obtains a pen register, it can only see the phone number that a person called; nothing indicates the contents of the phone call. A web history log, on the other hand, contains the websites that an individual visits; from there, the government agent could look at the visited website. For example, if an agent looked at a target's pen register, it could only hope to investigate that number and merely guess the contents of the call. With a website, an agent could see that a target accessed a website about how to make a bomb and then go to the site and view the content (Ditzion, 2004, p. 1338-1339).

E-mail presents a similar problem. While it is in like postal mail, legally, it still falls under the pen register umbrella. Legally, this even included the contents of the email until the Ninth Circuit court ruled in Worshak v. United States that Internet subscribers have a reasonable expectation of privacy in the contents of emails despite the fact that it passes through an ISP's server (Garlinger, 2009, p. 1142). The identifying information (such as subject lines and sender/recipient information), however, is not protected by the Fourth Amendment. Courts reason that the identifying information in an email is like pen register on a phone because it does not reveal the context of the email itself. Ditzion, however, argues that there are major differences between pen registers and email identifying information. Unlike phone numbers, email addresses "in general tend to be more person-specific than phone numbers." For instance, a phone number could be from a public phone booth, but an email almost always is sent and received from respective private email accounts. Furthermore, it is uncertain whether email attachments (that could include sensitive documents) and subject lines constitute email

identifying information or context (Garlinger, 2009, p. 1341). While it was in use Carnivore, reportedly considered the “To” and “from” fields to be identifying information, while subject lines were considered context; attachments were not part of that discussion (Garlinger, 2009,p. 1342). While these intercepting programs may target identifying information, Ditzion commented that content and identifying information is almost inseparable (Ditzion, 2004, p. 1336). The Court in Smith denied to give Fourth Amendment protection for pen registers for two reasons: because it was information voluntarily handed over to third parties and because a pen register did not reveal the contents of a phone call. The second prong of Smith is faulty, then, when applied to Internet communications.

Finding a Reasonable Expectation of Privacy

The analogy of pen registers and Internet surveillance is deceptive. It appears that the Smith line of cases (Smith, Miller, and Guest) be controlling precedent for Internet surveillance. In Smith, the Court ruled that the Fourth Amendment did not apply for two reasons. First, Mr. Smith had no expectation of privacy in the numbers he dialed because he had to have know that the phone company viewed the phone numbers for routing and billing purposes (Smith v. Maryland 1979, p. 724). Second, the pen register could not be considered a search because the pen register did not record the contents of the call, but merely the routing information (Smith v. Maryland 1979, p. 741). While the Smith precedent may have a few modifications when applied to Internet surveillance, such as giving Fourth Amendment protection to the content of emails in Worshak, it is still a guiding precedent for Internet surveillance. As mentioned, earlier, however, information that is sought in the domestic surveillance program is much more telling than a phone number. For example, an agent viewing the web history of a target can easily view what

sites the target has visited. A phone number, on the other, almost tells nothing about the subject of a call. If all this is true, cannot Smith be a fair and reliable precedent for Internet surveillance. To determine that we must answer two questions: First, Is there a reasonable expectation in Internet activity; Second, if so, what is the most appropriate way to collect such information?

The test of a “reasonable expectation of privacy” came from Justice Harlan’s concurring opinion in Katz v. United States. The majority in the case ruled that the government must obtain a warrant before placing a wiretap. Harlan, while agreeing with the majority, suggested a test to determine when the government must obtain a warrant for conducting electronic surveillance. Harlan wrote:

As the Court’s opinion states, “the Fourth Amendment protects people, not places.” . . .

My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, the expectation be one that society is prepared to recognize as “reasonable” (Katz v. United States 1967, p. 516).

Subsequently, courts have adopted this two-fold test to determine whether the Fourth Amendment applies to a particular case. Smith, in fact, exclusively relies on Katz to determine whether a pen register is unreasonable search (Smith v. Maryland 1979, p. 740). Therefore, it seems appropriate to use Harlan’s Katz test to determine if the domestic surveillance program violated the Fourth Amendment.

The district court in Doe v. Ashcroft agreed that the Katz test might be more relevant when it comes to electronic surveillance. The judge, however, refused to rule that the Terrorist Surveillance Program violated individual’s Fourth Amendment rights because of the clear Smith precedent. Judge Marrero (2004), in fact, directly compares the Katz case with Doe:

A person who signs onto a 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 legal process (Doe v. Ashcroft 2004, p. 510).

Marrero (2004) further noted that Smith might be an inappropriate precedent because “Internet records of the type obtained via a §2709 NSL could differ substantially from transactional bank or phone records (p. 509).

If the Katz precedent is more appropriate it is important how to determine whether a search is reasonable. By itself, Harlan’s “reasonable expectation” test is somewhat vague; how does one determine whether a search is reasonable? A year after Katz, the Supreme Court clarified Harlan’s rule. In Terry v. Ohio (1968), a case involving a street pat-down of a suspicious individual, the court ruled “there is ‘no ready test for determining reasonableness other than by balancing the need to search (or seize) against the invasion which the search (or seizure) entails’”; Slobogin (2007) called this the “proportionality principle” (Slobogin, 2007, p. 22). He explains this principle in full:

proportionality . . . is built on two propositions: (1) the interest the Fourth Amendment protects is security from unjustified government infringement on individuals’ property, autonomy (in the sense of ability to control one’s movements), and privacy; and (2) the greater the threat to that security, the greater justification the government should have to show (p. 23).

Indeed, the Court in Smith ruled that pen registers were not a search not only because Smith voluntarily gave that information to the phone company when he dialed those numbers, but also because a list of phone numbers is fairly unobtrusive compared to a wiretap.

Given the proportionality principle, should Internet surveillance be given Fourth Amendment protection? The answer depends on whether there is a reasonable expectation of privacy in Internet communication. People, of course already have a reasonable expectation of privacy in their homes from unwarranted government searches. The Supreme Court traditionally ruled that the government may not enter one's home without a judicial warrant. The Court, in Kyllo v. United States (2001) has even gone far as barring the thermal scanning of a home in search of indications that the occupants were growing marijuana inside of their home (Slobogin 2007, p. 16). The issue, however, is complicated when one broadcasts to the outside world within home. For example, the Court in Katz stated, "what a person knowingly exposes to the public, even in his own home or office, is not subject of Fourth Amendment protection" (Katz v. United States 1967, p. 351). For example, if a person grew a marijuana plant on their front porch many would agree that there would be no reasonable expectation of privacy (and therefore no Fourth Amendment protection). Phone calls, of course, are glaring exception in this case. While it is a broadcast outside of the home, the Court has clearly ruled that there is a clear expectation of privacy in the *contents* of a phone call largely because of the importance the telephone has in everyday life (Smith v. Maryland 1979 p. 751).

Like a phone call, the Internet has become a staple in the home for communication. Once again, the problem seems to stem from the third party precedent from Miller. Of course, not everything given voluntarily to a third party loses Fourth Amendment protection (like a phone call, a piece of mail, or the content of an email). To put the intrusiveness of electronic

surveillance in perspective, Slobogin (2007) surveyed Americans asking them to rank the intrusiveness of twenty-five different searches scale from 1 to 100 ⁶. Out of the twenty-five scenarios, a bedroom search ranked as the most intrusive with a mean score of 81.5. Interestingly enough, seizure of bank records ranked as the second most intrusive with a mean score of 80.3. Search of e-mail addresses ranked fifth most intrusive with a mean score of 77.1. Web sites visited ranked eighth most intrusive with a mean score of 74.4. The least intrusive personal electronic surveillance, according to the survey, was data mining of phone records with a mean score of 50.0 (Slobogin 2008, p. 184). Slobogin noted:

Web sites visited, credit card purchases, and pharmacy and bank records. These types of transaction surveillance are all ranked as more intrusive than a pat down and about as intrusive as either a car search (scenario 19) or a search of a bedroom (scenario 25), both of which require probable cause (p. 185).

Given this survey and general societal views, it appears that society recognizes that there is a reasonable expectation of privacy in Internet communication. In order to determine whether the domestic surveillance program passes Fourth Amendment muster, the other part of Harlan's Katz test must be answered: Are the means of the search justified?

An Important Means to an End

To determine if the search is justified, the need for surveillance must outweigh the intrusiveness of the search. Evidently, most of the American people are mixed on the need for the Terrorist Surveillance Program. In a May 11, 2006 Washington Post-ABC News poll⁷, when Americans were asked "What do you think is more important right now - (for the federal

⁶ For full survey results, see Appendix 1

⁷ For full survey results, see Appendix 2

government to investigate possible terrorist threats, even if that intrudes on personal privacy); or (for the federal government not to intrude on personal privacy, even if that limits its ability to investigate possible terrorist threats)?, sixty-five percent answered “investigate threats” compared to the thirty-one percent who answered “respect privacy.” Furthermore, when asked If you found out that the NSA had a record of phone numbers that you yourself have called, would that bother you, or not? IF YES: Would it bother you a lot, or just somewhat?” sixty-six percent answered “No” it would not bother them compared to a net of thirty-four percent who answered “Yes” it would bother them (24% saying “A lot” while 10% saying “Somewhat”) (Washington Post-ABC News Poll” 2006). It seems that most Americans, in this survey at least, appear to recognize the need of the program to defend the country. A Newsweek poll conducted the same day, however, stated that fifty-three percent of Americans believed the Terrorist Surveillance Program was a violation of privacy rights (Hosenball and Thomas, 2006, p. 22).

However, John Yoo, believed public opinion does not matter to determine if the search is justified. Yoo, a legal counsel early in the Bush administration, noted “the government’s interest . . . [outweighs] the individual’s privacy interest, and that in this regard ‘no governmental interest is more compelling than the security of the Nation.’” The Supreme Court recognized the principle in Haig v. Agee (1981) (Offices of Inspectors General, 2009, p. 13). No one can doubt the importance of national security. In the Age of Information, terrorist plots can unfold quickly and the government must act quickly to stop those plots. Just because there is a great need for the search, however, does mean that government agents can subvert all Constitutional protections. For example, a bomb threat in a major city does not justify government agents to tear through every single home and office building at will. While this is an extreme example, Yoo implicates

that national security trumps any sort of privacy interest. Just because there is a great need for the search does not mean it can be conducted without limitations.

The Fourth Amendment, however, is flexible. While the content of phone conversations and the contents of emails are given Fourth Amendment protection, it does not mean that they require the same legal authorization. Different searches require different forms of authorization. For example, a wiretap on a private telephone line or the search of one's home requires that the government show probable cause that the suspect is committing or has committed a crime. On the other hand, the government needs only to prove relevance to an ongoing investigation to obtain a subpoena that requires businesses to surrender relevant information (Slobogin 2007, p. 186-187).

The Terrorist Surveillance Program, however, presents an interesting problem in Fourth Amendment law. Originally, all surveillance focused on a single target (target-driven searches). The Internet now, however, allows the government to easily conduct vast data sweeps in certain targeted areas (event-driven searches) or even searches for certain suspects given certain criteria (match-driven searches), although the Supreme Court has yet to rule on the Constitutionality of suspicionless event-driven searches (Slobogin 2007, p. 217). The Supreme Court has allowed some cases of generalized suspicion in cases where the search itself is fairly unobtrusive like a road stop to check for drunk drivers (Slobogin 2007, p. 41). The Internet, though, complicates Fourth Amendment analysis. Some things on the Internet, like the content of emails, have high expectations of privacy while posting a message on an public message board is given substantially less privacy protection.

Rather than further complicate the already messy Fourth Amendment case law, Slobogin suggests a series of different approaches given the nature of the search. For target-driven

searches (the traditional approach), Slobogin (2008) suggests three tiers of searches. The bottom tier would apply to “corporate records and most public records (for example, criminal and real estate records).” The bottom tier would require government officials to show a judge that there is a legitimate interest in order to obtain a warrant. The middle tier “would involve target-driven efforts to obtain records that are quasi-private because they contain information considered less personal (for example, power consumption records, high school records).” The middle tier would require that government officials show that there is a “reasonable suspicion” that the evidence would prove that target has committed or is committing a crime. The high tier “would include target-driven attempts to obtain records containing the most personal information (for example, bank records and phone and ISP logs).” The high tier would require that government officials show a judge that there is “probable cause” that evidence obtained would show that the suspect is or has committed a crime. Match-driven searches “would depend not on the nature of the records searched but on the nature of the action the government contemplates taking when a match occurs.” (p. 337). Event-searches, however, present an interesting case. Some searches, targeted in a certain area because of a threat could range the spectrum from the non-intrusive (like information of traffic patterns) to the highly intrusive such as personal financial information. Because of this variety, then, Slobogin (2008) suggests that there be a blanket “reasonable suspicion” that the information sought would produce information would show evidence of a potential attack (p. 339).

Whatever the standard may be, the power of the Fourth Amendment relies on judicial oversight. As the Internet becomes more ingrained in society, the reach of government surveillance becomes more intrusive. While it might be practically impossible to impose a blanket “probable cause” on all searches, at the same time, no judicial oversight on intrusive

searches undermines the founding principles of the nation. No court has yet stated that the Terrorist Surveillance Program violates individuals' Fourth Amendment rights. Applying Harlan's Katz test, however, it appears that the program may not pass Fourth Amendment muster. It is plain to see that in at least private Internet communications such as email and browsing history, there is a reasonable expectation of privacy. Because there is a reasonable expectation, the government can only invade that area of privacy only when the search is reasonable. While national security may be a grave justification of a search, current lack of some form of judicial oversight is not reasonable in light of the intrusiveness of the search.

Jackson's Test

Despite the controversy of the domestic surveillance program, President Bush and President Obama have defended their ability to authorize and conduct the program in the face of clear Congressional opposition. While the Foreign Surveillance Intelligence Act gave clear standards for conducting foreign surveillance that implicated Americans, President Bush believed that his prerogative as commander-in-chief trumped any Congressional mandate. Furthermore, the data mining of both administrations that has been unquestionably intrusive has been conducted without any sort of Congressional mandate. These two components of this program face two different and important Constitutional questions: 1. Whether the President may act against Congressional will; and 2. Whether the President can act without authority from Congress.

The beginning of either answer lies in Justice Jackson's three-part test in his concurring opinion in Youngstown Sheet & Tube Co. v. Sawyer (1952). He ranks three situations of Presidential power in the opinion. The President is the most powerful, Jackson argued, when he

or she “acts pursuant to an express or implied authorization of Congress . . . for it includes all that he possesses in his own right plus all that Congress can delegate” (p. 635). These cases typically pass Constitutional muster: “it usually means that the Federal Government as an undivided whole lacks power.” The President is less powerful, when “the President acts in absence of either a Congressional grant or denial of authority [where] he can only rely upon his own independent powers.” In these cases, however:

here is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain. Therefore, Congressional inertia, indifference or quiescence may sometimes, at least as a practical matter, enable, if not invite, measures on independent Presidential responsibility (p. 637).

Finally, Jackson argues, the President is the least powerful when he or she “takes measures incompatible with the expressed or implied will of Congress . . . for then he can rely only upon his own Constitutional powers minus any Constitutional powers of Congress over the matter” (p. 637). Here:

Courts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject. Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our Constitutional system (p. 637-638).

Using this test, Justice Jackson reasoned that President Truman went beyond his authority as commander-in-chief when he seized steel mills in 1952 across the country in order to prevent a workers’ strike (p. 638).

The Supremacy Argument

Using Jackson's test, then, did President Bush go beyond his Article II powers? While Bush later acquiesced to Congress after a political firestorm, maintained that he had authority to unilaterally authorize the Terrorist Surveillance Program. Ordering the electronic surveillance of Americans without consulting the Foreign Intelligence Surveillance Court blatantly violated FISA; however, President Bush argued that he had the authority as commander-in-chief to override FISA in the "interception of international communication of people with known links to al Qaeda" (Young, 2007). In the early part of the administration, John Yoo proposed that to President Bush that he did have the authority to override FISA. In fact, Yoo advised the President that FISA was an unconstitutional infringement on his Article II powers as commander-in-chief. For Yoo, the ultimate test for the program was the Fourth Amendment (Offices of Inspectors General, 2009, p. 11). Under the Fourth Amendment framework, then, Yoo reasoned that the program conducted searches reasonably, because the need for the search (national security) outweighed the intrusiveness of the program (Offices of Inspectors General, 2009, p. 12).

Other scholars, such as Professor Robert Turner from the University of Virginia School of Law also argue that FISA is an infringement on Presidential power. He, and many other, scholars argue that Youngstown is good precedent for domestic cases, but United States v. Curtiss-Wright Export Corp. (1936) is the appropriate precedent for the Terrorist Surveillance Program. In this case, the Supreme Court ruled that the President is the "sole organ" of foreign affairs and that Congress has no authority to infringe on that right (United States House of Representatives (Part I), 2007, p. 33). Cases before FISA upheld this precedent when it came to foreign surveillance. In 1965, the Fifth Circuit Court of Appeals allowed the Attorney General to

use warrantless wiretaps for foreign intelligence; the case cited the Curtiss-Wright case for the supremacy of the President in foreign affairs (Addicott and McCaul 2007, p. 52-53). The Third Circuit did the same in 1974 in United States v. Butenko when it allowed warrantless electronic surveillance “so long as the primary purpose of the activity was to obtain foreign intelligence” (Addicott and McCaul 2007, p. 53).

The courts continued to uphold the President’s authority to conduct foreign surveillance even after FISA. The Fourth Circuit Court of Appeals ruled in United States v. Truong (1980) that the President had the authority to conduct foreign surveillance without the permission of FISA (United States House of Representatives, 2007, p.44). Furthermore, the FISA Court of Review, the special appeals court of the FISC, ruled in In re Sealed Case (2002), that “the President [has the] inherent authority to conduct warrantless searches to obtain foreign intelligence information” (United States House of Representatives, 2007, p. 45). Turner noted that United States v. United States District Court (1972) explicitly stated that the government could not conduct explicitly domestic surveillance; the Court left sole discretion of foreign surveillance to the President (United States House of Representatives, 2007, p. 41). Turner makes a distinction that the two cases show that the President has absolute authority (foreign surveillance) and limited authority (domestic surveillance) to authorize warrantless wiretapping despite Congress’ action. The problem with Turner’s logic, however, is that President Bush’s domestic surveillance program may allegedly target foreign agents, but it at times implicates Americans in the search net. Turner’s simple dichotomy ignores the large ambiguity of the program.

The FDR Precedent Revisited

According to Jackson's test, because the President acted in the face of Congressional opposition, the President must rely on his argument that his role as commander-in-chief and the "sole organ" of foreign affairs grants him the Constitutional authority to execute the Terrorist Surveillance Program. In the absence of explicit Constitutional authority, a clear precedence of Presidential action is always a strong argument for validating Presidential actions. The Bush administration relies on Franklin Roosevelt's use of warrantless wiretaps for his administration to support the Constitutionality of the President's actions. As mentioned in Chapter 1, FDR actively ignored the Nardone rulings, which required a warrant for a wiretap; FDR believed his commander-in-chief powers allowed him to make an exception for national security cases. Caplan and Katyal (2008), however, noted that FDR's action did not come without controversy; which, for them, hardly qualifies FDR's actions as a clear indication of Presidential authority. The authors suggest a few guidelines to determine whether a controversial executive act should have force.

- (a) whether [the executive act] was done openly and was the subject of public debate; (b) whether it was approved—or at least not rejected—by the legislature at the time; (c) whether it was approved by other Presidents, legislatures, and analysts in subsequent time periods; and (d) whether it concerns a practice as to which the Constitution does not offer a clear guide (p. 146).

Using this rubric, then, the authors believed that the FDR precedent had no force. First, FDR authorized warrantless wiretaps without public knowledge. Second, he authorized the wiretaps in the face of clear legislative opposition; Congress made wiretaps illegal without a warrant in the 1934 Communications Act (p. 146). Third, "as a matter of Constitutional governance, it is

exceptionally dangerous to vest a President with the power to break the laws, at least at a time when Congress can act” (p. 147). Furthermore, FDR’s unilateral authorization of wiretapping was unprecedented in peacetime. While President Lincoln wiretapped telegraph lines, it was done in clear absence of Congressional statute. It would be irresponsible to grant the President the authority to violate law he so chose during peacetime. Finally, the Constitution clearly does not provide a clear guide in either the FDR precedent or the Terrorist Surveillance Program. The lack of explicit Constitutional authority or implicit Constitutional authority from a firm precedent eliminates any legitimate argument that the President had the authority to unilaterally authorize the Terrorist Surveillance Program.

An Ambiguous AUMF Argument: The Last Hope

The Bush Administration, however, contended that Congress in fact did give them the authority to conduct the Terrorist Surveillance Program. In the December 19, 2005 conference after the *New York Times* leak, President Bush asserted that his commander-in-chief powers gave him the authority to override FISA, and therefore gave him the authority to conduct the program. President Bush cited the Authorization to Use Military Force (AUMF) as a Congressional mandate to authorize the program (Fisher 2008, p. 292). The statute in question, discussed at length in Chapter 2, mentions nothing explicitly about domestic surveillance, but merely authorizes the President to use armed force against those responsible for the September 11 attacks (p. 393). Lawson noted that while the AUMF may regulate military intelligence gathering, it is difficult to connect it to “the monitoring of non-battlefield communications” (Lawson 2008, p. 379).

Additionally, Dworkin, et. al.(2006)—a team of prominent legal scholars and former government officials—warn that the President may not act on such ambiguous terms. Dworkin et al. believe in order for the President to violate clear laws governing domestic surveillance, he must have *clear* authority from either the Constitution or Congress itself. They note that while the AUMF is far from clear, Congress clearly legislated electronic surveillance. Statues such as FISA and the Electronic Communications Privacy Act of 1986, among others, provide clear guidelines for the program’s surveillance; therefore, it is difficult to throw out those laws unless by a clear directive from Congress. Justice Felix Frankfurter in Youngstown chided President Truman for also acting on ambiguous terms:

It is one thing to draw an intention of Congress from general language and to say that Congress would have explicitly written what is inferred, where Congress has not addressed itself to a specific situation. It is quite impossible, however, when Congress did specifically address itself to a problem, as Congress did to that of seizure, to find secreted in the interstices of legislation the very grant of power which Congress consciously withheld. To find authority so explicitly withheld is...to disrespect the whole legislative process and the Constitutional division of authority between President and Congress (Youngstown Sheet & Tube Co. v. Sawyer, 1952, p. 609).

There is no argument the President may act on an ambiguous statute when existing statute already prohibits that action. Given this and the earlier argument that the President has no Constitutional authority to defy Congress, it is clear that President Bush never had the authority to authorize and execute the Terrorist Surveillance Program.

The Verdict

The Terrorist Surveillance Program is an interesting case in Constitutional law. Jumbled Fourth Amendment case law has left the Internet exposed to outdated surveillance law. Simply applying the same legal standard for all electronic communications ignores the difference between forms of electronic communication. The Terrorist Surveillance Program violated the Fourth Amendment in the spirit of the law, but not of the law itself. The program abides by current laws and Fourth Amendment case law, but an examination of the program reveals that it clearly violates Justice Harlan's test in Katz, the root precedent of modern Fourth Amendment case law. Applying Harlan's test to the Terrorist Surveillance Program, it is clear to see that there is a reasonable expectation in Internet communications and that the search itself is unjustifiably intrusive.

The case is clearer when it comes to the President's power to execute the program. When the program began, President Bush clearly violated standing laws governing domestic surveillance such as FISA and the Electronic Communication Privacy Act. The interception of phone and Internet data directly violated Congressional statute. According to Jackson's Youngstown test, the President may only violate the will of Congress only when he or she has the clear Constitutional authority to do so. An examination of President Bush's Constitutional arguments, however, reveal that there is no clear Constitutional authority for electronic surveillance. Therefore, President Bush did not have the authority to override laws governing electronic surveillance.

Conclusion

The Terrorist Surveillance Program is most likely just the beginning of electronic surveillance in the age of the Internet. Over the last decade, the personal computer and the cell phone have made electronic communication a central part of American society. As the role of electronic communication increases, it is becoming difficult to stop the flow of personal information into the hands of both corporations and the Federal government. This trend is not likely to reverse. Programs such the Terrorist Surveillance Program then will become ever more intrusive in a digitalized world; however, this does not eliminate the possibility of such programs. Because of the grave implications, it is necessary to reach some compromise in order to preserve both the privacy rights of individuals and an effective means to protect national security.

The Terrorist Surveillance Program has four stages. First, the public must actually disseminate the information sought by the Terrorist Surveillance Program. Second, the government must actually obtain that data. Third, government officials must analyze that information. Fourth, analysts must apply that information to stop terrorist plots and to prosecute offenders. The key to preserving privacy rights on the Terrorist Surveillance Program is to regulate government action at each of these stages.

Looking at the first stage, it is very difficult to stop or even regulate what is disseminated to the public. Limiting the flow of personal information in the marketplace would require massive changes in the way Americans conduct business. It is unreasonable to stop the flow of personal information third parties. To do so would disrupt many key factors of the modern economy.

The second stage, however, has possible solutions. The Terrorist Surveillance Program collects information in two ways: through intercepting programs such as Carnivore and Narsus and through National Security Letters. Limiting interception is a promising solution. One solution is to leave Internet communications anonymous: blocking the Internet Protocol addresses when transferring information to the government could be the best possible solution to this problem. The government would still be able to obtain information it would need for a functioning database and the people would have the right to keep their communications anonymous. The same can apply for stored information on third party servers. Once the database would show a possible terrorist attack, the government then could ask for judicial approval to obtain personalized information. Changing interception equipment would only implicate individual privacy when there is a national security need.

The other part of the collection process, National Security Letters, should change in a similar way. Information currently sought by a NSL, such as personal Internet logs and emails, is too intrusive. Congress should remove Internet communications from the reach of an NSL. Judicial oversight is necessary to obtain information that has a reasonable expectation of privacy. I discussed in Chapter 4 that Internet communication do have this expectation of privacy and therefore should be subject to Fourth Amendment protection. If Congress refuses to limit the reach of NSLs, however, there must at least be some judicial oversight in the NSL process. Fourth Amendment protections can remain intact if NSLs are limited by judicial oversight; the crux of the Fourth Amendment is judicial oversight to determine whether searches are reasonable.

If changes are implemented in the second stage, little needs to be changed in the third stage. Analysts can still operate if the recommended collection methods are implemented. The

purpose of the second stage changes are not to limit what can be obtained, but rather to ensure that such collection methods are done reasonably.

The final stage, prosecution, would need certain changes. Traditional Fourth Amendment law requires a warrant to obtain private papers that may be incriminating; the same should be applied to Internet communications. To obtain the most private information online (such as banking information, emails, and Internet logs), a government agent must prove probable cause that such information would prove that an individual is committing a crime in order to collect that information. Slobogin's tiered approach, mentioned in Chapter 4, provides a clear guide for different standards of authorization for different tiers of information. Ultimately, the Terrorist Surveillance Program must be limited to conducting surveillance to prevent terrorist plots, not to prosecute individuals.

The best solution is often the easiest solution. Legal scholars and the Obama Administration should sit down and decide a solution that sufficiently protects individual liberty in a way where it is the least disruptive to conducting surveillance. This process should not lie solely with the President. Congress must work with the President to find a sufficient solution to the problem. The public must be clearly informed of the changes to the Terrorist Surveillance Program in order to establish the legitimacy of the program. The public must be aware of what information can be collected, how it is collected, and why it is collected. Establishing this public dialogue is essential to future success of the program. The easiest way to accomplish this is for the President to directly talk to the American people about the program and send a clear statement about what the program can and cannot do. Ironically, the Internet may be the best place to start this dialogue.

Despite its flaws, the Terrorist Surveillance Program should not be dismantled, but rather changed. In a world where terrorism depends on electronic communication, the government must have some tool to stop terrorist attacks before they happen. National security, after all, is the most sacred duty of government. This does not mean, however, that it can violate our Constitutional principles in order to achieve that end. It is possible, and necessary, to reframe the Terrorist Surveillance Program to meet minimal Constitutional protections.

The United States of America has been through perilous times. In this time of great uncertainty, the American people must not panic and give up on our founding principles. The United States Constitution sought to protect individual liberty from a tyrannical government. If we endanger those values to fight a protracted war of terror, there will be eventually nothing left to defend.

Appendix

Appendix 1: United States Constitution, Amendment I

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

Appendix 2: Slobogin 2008, p. 335

Scenario	Mean	Confidence Intervals
1 <i>Roadblock</i>	30.2	±7.5
2 Airplane passenger lists (event-driven)	32.4	8
3 Store patron lists (event-driven)	34.1	7.5
4 Criminal/traffic records	36.2	7
5 Anonymous phone, credit card, and travel records (event-driven)	38.5	7
6 Corporate records	40.6	7
7 Real estate records	45.5	8
8 <i>ID check and questioning during brief stop</i>	49.1	8
9 Club membership records	49.5	8
10 Phone records (event-driven)	50.0	8
11 Electricity records	57.5	8
12 High school records	58.3	9
13 Phone, credit card, and travel records (event-driven)	59.7	8
14 Record of specific phone call	59.8	7.5
15 List of food purchases	65.3	7.5
16 <i>Patdown</i>	71.5	7.5
17 Phone records	74.1	7.5
18 Websites visited	74.4	8
19 <i>Search of car</i>	74.6	7
20 Credit card records	75.3	7.5
21 Email addresses sent to and received from	77.1	8
22 Pharmacy records	78.0	7.5
23 Use of snoopware to target subject	79.0	8
24 Bank records	80.3	7.5
25 <i>Bedroom search</i>	81.2	6.5

Note: Scenarios not involving transaction surveillance appear in italics. These findings are based on a survey administered to seventy-six members of the Gainesville, Florida jury pool, randomly selected from a list composed of all residents who have a driver's license or identification card. See Fla Stat Ann § 40.011 (West 2007).

Appendix 3: "Washington Post-ABC News_Poll" May 12, 2006

http://www.washingtonpost.com/wp-srv/politics/polls/postpoll_nsa_051206.htm

4. Do you approve or disapprove of the way Bush is handling protecting Americans' privacy rights as the government investigates terrorism?

	Approve	Disapprove	No opinion
5/11/06	51	47	2

44. What do you think is more important right now - (for the federal government to investigate possible terrorist threats, even if that intrudes on personal privacy); or (for the federal government not to intrude on personal privacy, even if that limits its ability to investigate possible terrorist threats)?

	Investigate threats	Respect privacy	No opin.
5/11/06	65	31	4
1/8/06	65	32	3
9/7/03*	73	21	5
9/8/02	78	18	4
6/9/02	79	18	3

45. It's been reported that the National Security Agency has been collecting the phone call records of tens of millions of Americans. It then analyzes calling patterns in an effort to identify possible terrorism suspects, without listening to or recording the conversations. Would you consider this an acceptable or unacceptable way for the federal government to investigate terrorism? Do you feel that way strongly or somewhat?

	----- Acceptable -----			----- Unacceptable -----			No
	NET	Strongly	Somewhat	NET	Somewhat	Strongly	opin.
5/11/06	63	41	22	35	11	24	2

46. If you found out that the NSA had a record of phone numbers that you yourself have called, would that bother you, or not? IF YES: Would it bother you a lot, or just somewhat?

	-----Yes-----				No	No opin.
	NET	A lot	Somewhat			*
5/11/06	34	24	10	66		

47. Do you think it is right or wrong for the news media to have disclosed this secret government program?

	Right	Wrong	No opin.
5/11/06	56	42	1

Works Cited

- Addicott, J. & McCaul, M. (2007). The Protect America Act of 2007: A Framework for Improving Intelligence Collection in the War on Terror. *Texas Review of Law and Politics*, 13, 44-71.
- Authorization for Use of Military Force. (2001) Pub. L. 107-40.
- Bellis, M. (2010). The History of the Electric Telegraph and Telegraphy. *About.com*. Retrieved November 12, 2010, from <http://inventors.about.com/od/tstartinventions/a/telegraph.htm>
- Boyd v. United States. (1886). 116 U.S. 616. Sup Ct. of the US.
- Brandeis, L. and Warren, S (1890). The Right to Privacy. *Harvard Law Review*, 4
- Brian, M. (2000). How Telephones Work. *Howstuffworks.com*. Retrieved November 12, 2010, from <http://communication.howstuffworks.com/telephone1.htm#>
- Broache, A. and McCullagh, D. (2006a). Backer of ISP snooping slams industry. *cnet.com*. Retrieved November 12, 2010, from http://news.cnet.com/Backer-of-ISP-snooping-slams-industry/2100-1028_3-6068339.html?tag=mncol;txt
- Broache, A. and McCullagh, D. (2006b). Gonzales: ISPs must keep records on users. *cnet.com*. Retrieved November 12, 2010, from http://news.cnet.com/Gonzales-ISPs-must-keep-records-on-users/2100-1028_3-6117455.html?tag=mncol;txt
- California v. Ciraolo. (1986). 476 U.S. 207. Sup. Ct. of the US.
- Caplan, R. & Katyal, N. (2008). The Surprisingly Stronger Sase for the Legality of the NSA Surveillance Program: The FDR Precedent. *Georgetown Law Faculty Working Papers*. 102-156.
- Cauley, L. (2006, May 11). NSA has massive database of Americans' phone calls. *USA Today*.

Retrieved November 12, 2010, from http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm

Diffie, W. & Landau, S. (2007). *Privacy on the Line*. Cambridge, MA: MIT Press

Ditzion, R. (2004). Electronic Surveillance in the Internet Age: The Strange Case of Pen Registers. *American Criminal Law Review*, 41, 1322-1352.

Doe v. Ashcroft. (2004). 334 F. Supp. 2d. 471. US Dis. Ct. for the S. Dis. of NY.

Dworkin, R., Sullivan, K., Tribe, L, Cole, D., Bradley, C. et al. (2006). On NSA Spying: A Letter to Congress. *The New York Review of Books*. Retrieved November 12, 2010 from, <http://www.nybooks.com/articles/archives/2006/feb/09/on-nsa-spying-a-letter-to-congress/>

Foerstel, H. (2008). *The Patriot Act: A Documentary and Reference Guide*. Westport, Conn: Greenwood Press.

Foreign Intelligence Surveillance (1978) Act. Pub. L. 95-511. 25

Fisher, L. (2008). *The Constitution and 9/11*. University Press of Kansas.

Garlinger, P. Note: Privacy, Free Speech, and the Patriot Act: First and Fourth Amendment Limits on National Security Letters. *New York University Law Review*, 84, 1105-1147.

Griswold v. Connecticut. (1965) 381 U.S. 479. Sup Ct. of the US.

Guest v. Leis. (2001). 255 F.3d 325. U.S. App 6th Cir.

Hosenball, M and Thomas. (2006, May 22). Hold the Phone: Big Brother knows whom you call. Is that legal, and will it help catch the bad guys? *Newsweek*, 22

Katz v. United States. (1967). 389 U.S. 347. Sup Ct. of the US.

Konrad, R. (2000, November 16). New documents shed more light on FBI's "Carnivore."
cnet.com. Retrieved

November 12, 2010, from http://news.cnet.com/New-documents-shed-more-light-on-FBIs-Carnivore/2100-1023_3-248762.html?tag=mncol;txt

Kyllo v. United States. (2001). 533 U.S. 27. Sup Ct. of the US.

Lawson, G. (2008) What Lurks Beneath: NSA Surveillance and Executive Power. *Boston University Law Review*, 88, 375-393.

Lichtblau, J. and Risen, E. (2005, December 16). Bush Lets U.S. Spy on Callers Without Courts.
New York Times. Retrieved November 12, 2010, from
http://www.nytimes.com/2005/12/16/politics/16program.html?_r=1

McCullagh, D. (2005, June 16). Your ISP as New watchdog. *cnet.com* Retrieved November 12, 2010, from http://news.cnet.com/Your-ISP-as-Net-watchdog/2100-1028_3-5748649.html?tag=mncol;txt

McCullagh, D. (2007, February 6). GOP revives ISP-tracking legislation. *cnet.com* Retrieved November 12, 2010, from http://news.cnet.com/GOP-revives-ISP-tracking-legislation---page-2/2100-1028_3-6156948-2.html?tag=mncol

Nakashima, E. (2010, July 29). White House proposal would ease FBI access to records of Internet activity. *The Washington Post*. Retrieved November 12, 2010, from
http://www.washingtonpost.com/wp-dyn/content/article/2010/07/28/AR2010072806141.html?nav=rss_email/components

Nardone v. United States [Nardone I]. (1937). 302 U.S. 379. Sup. Ct. of the US.

Nardone v. United States [Nardone II]. (1939). 308 U.S. 338. Sup. Ct. of the US.

O'Harrow, R. *No Place to Hide*. New York: Free Press, 2005.

- Offices of Inspectors General. (2009). *Unclassified Report on the President's Surveillance Program*. Washington, DC: U.D. Government Printing Office
- Olmstead v. United States. (1928). 277 US 438. Sup Ct. of the US.
- Quint, P. (1981). The Separation of Powers under Nixon: Reflections of Constitutional Liberties and the Rule of Law. *Duke Law Journal*, 1, 1-70.
- Reardon, M. (2006, May 15). Verizon sued for alleged NSA cooperation. *cnet.com* Retrieved November 12, 2010, from http://news.cnet.com/Verizon-sued-for-alleged-NSA-cooperation/2100-1036_3-6072483.html?tag=mncol;txt
- Safire, W. (2002). You Are a Suspect. *New York Times*. Retrieved November 12, 2010, from <http://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html>
- Slobogin, C. (2007). *Privacy at Risk: The New Government Surveillance and the Fourth Amendment*. Chicago: University of Chicago.
- Slobogin, C. (2008). Government Data Mining and the Fourth Amendment. *The University of Chicago Law Review*, 75, 317-341
- Smith v. Maryland. (1979). 442 U.S. 735. Sup. Ct. of the US.
- Tyson, J. (2001) How Internet Infrastructure Works. *Howstuffworks.com* Retrieved November 12, 2010. from <http://computer.howstuffworks.com/internet/basics/internet-infrastructure.htm>
- United States House of Representatives (2007). *Warrantless Surveillance and the Foreign Intelligence Surveillance Act: The Role of Checks and Balances in Protecting America's Privacy Rights (Part I)*. Washington, DC: U.D. Government Printing Office
- United States House of Representatives (2007). *Warrantless Surveillance and the Foreign*

Intelligence Surveillance Act: The Role of Checks and Balances in Protecting America's Privacy Rights (Part II). Washington, DC: U.D. Government Printing Office

United States House of Representatives. (2009). *USA Patriot Act*. Washington, DC: U.D. Government Printing Office

United States Senate (1976). *Select Committee to Study Governmental Operations with Respect to Intelligence Activities*. Washington, DC: U.D. Government Printing Office

United States v. Curtiss-Wright Export Corp. (1936). 299 U.S. 304. Sup. Ct. of the US.

United States v. Kennedy. (2000). 81 F. Supp. 2d 1103 U.S. Dist.

United States v. Miller. (1976). 425 U.S. 435. Sup. Ct. of the US.

United States v United States District Court. (1972). 407 U.S. 297. Sup. Ct. of the US.

Washington Post-ABC News Poll. (2006, May 12). *The Washington Post* Retrieved November 12, 2010 from, http://www.washingtonpost.com/wp-srv/politics/polls/postpoll_nsa_051206.htm

Young, R. (Executive Producer). (2007). *Frontline: Spying on the Homefront*. [Television Program]. PBS.

Youngstown Sheet & Tube Co. v. Sawyer. (1952). 343 U.S. 579. Sup. Ct. of the US.

Acknowledgements

I would like to thank my friends for all of their support despite my constant complaining about my Comp.

Specifically, I would like to thanks Lyndsay Steinmetz, the members of my apartment (“3 Girls, 1 Brett”) Kirsten Dean, Anna Rose Welch, and Ali Trunzo for helping me whenever I got stuck in a rut.

I would also like to thank Professor Brian Harward for all of his help developing this project.

Finally, I would like to thank my right arm for pulling double duty after I broke my left wrist in Late September