6-15-2007

The Evolution of Electronic Surveillance: Balancing National Security and Civil Liberties

Phillip Ryan Hussey

THE EVOLUTION OF ELECTRONIC SURVEILLANCE: BALANCING NATIONAL SECURITY AND CIVIL LIBERTIES

by

PHILIP RYAN HUSSEY

Under the Direction of Robert Howard

ABSTRACT

This paper examines the history of electronic surveillance for national security purposes within the United States and relates the statutory and constitutional law to the current, post September 11th practices. An extensive examination of the Foreign Intelligence Surveillance Court and the recently leaked, classified Terrorist Surveillance Program shows that the FISA Court, within its narrow jurisdiction, adequately accounts for constitutional standards, yet the TSP—including recent reforms—is in clear violation of constitutional and statutory law.

INDEX WORDS: Electronic surveillance, Wiretapping, FISA, Domestic spying

THE EVOLUTION OF ELECTRONIC SURVEILLANCE: BALANCING NATIONAL SECURITY AND CIVIL LIBERTIES

by

PHILIP RYAN HUSSEY

An Honors Thesis Submitted in Partial Fulfillment of the

Requirements for Graduation with Undergraduate Research Honors

in the College of Arts and Sciences

Georgia State University

2007

THE EVOLUTION OF ELECTRONIC SURVEILLANCE: BALANCING NATIONAL SECURITY AND CIVIL LIBERTIES

by

PHILIP RYAN HUSSEY

Honors Program Director: Dr. Robert Sattelmeyer

Electronic Version Approved:

Honors Program
College of Arts and Sciences
Georgia State University
May 2007

ACKNOWLEDGEMENTS

I would like to thank my faculty advisor, Dr. Howard, whose red pen constantly helped take this paper further. I would also like to thank the Georgia State University Honors Department for providing to students opportunities not found in the traditional classroom setting. Finally, I would like to thank my parents, Brian and Pam Hussey, for their ever constant support and encouragement.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

FISA:	Foreign Intelligence Surveillance Act
FISA Court:	Foreign Intelligence Surveillance Court
OIPR:	Office of Intelligence Policy Review
TSP:	Terrorist Surveillance Program
AUMF:	Authorization for the Use of Military Force
PATRIOT Act:	Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

INTRODUCTION

Throughout the history of the United States there exists a constant struggle between individual liberties and national security. Attacks from abroad often increase the need to strengthen national security, yet this increase leaves open the potential for government to erode certain freedoms. This includes the Fourth Amendment, which proclaims, "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated."[1] This particular protection continues to be the forefront in the struggle between national security and individual freedom. The Fourth Amendment symbolizes "the uniqueness of American freedom and the centrality of the concept of the rule of law and the sovereignty of the people."[2] Thus the Fourth Amendment is vital to the American system of democracy and it is necessary to keep the government from intruding, without cause, on the privacy of its citizens.

Yet intrusion is not always the simple act of government officials entering into private property. In recent history the protections found in the Forth Amendment have also adapted with changes in technology. Federal law enforcement officers have been able to use electronic surveillance as a tool to investigate citizens since the advent of electronic communication, and the legal community has adjusted its interpretation of the

[1] U.S. Constitution. Amend. IX.

[2] Samuel Dash. *The Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft.* (Rutgers University Press: New Brunswick, 2004), 6.

Fourth Amendment with the changing times. When a national crisis arises however, the desire for stronger national security often reopens the debate to what forms of electronic surveillance are acceptable.

The events following September 11th were no exception. In fact, recent events show that significant constitutional issues have arisen within the jurisprudence of electronic surveillance policy. On January 18, 2007, the Department of Justice announced that the National Security Agency's controversial, warrantless electronic surveillance program, often referred to as the Terrorist Surveillance Program, would be brought under the jurisdiction of the Foreign Intelligence Surveillance Court.[3] Some journalists asserted that this new announcement was an "an abrupt reversal by the administration" in their policies of electronic surveillance on domestic soil.[4] Yet after careful examination of the change in policy, it is clear that many questions still remain as to the constitutionality of the TSP. This paper will argue that the administration's policy does not end the statutory and constitutional violations of the TSP. This argument will be conducted in four steps: first, an extensive examination of the jurisprudence of electronic surveillance will be examined to lay foundation for the debate; second, it will be argued that an appropriate, constitutional balance was achieved with the passage of the Foreign Intelligence Surveillance Act and the subsequent establishment of the FISA Court; next, the constitutionality of the Terrorist Surveillance Program will be addressed; and finally, various solutions to bring electronic surveillance policy back into the realm of constitutionality will be suggested.

---

[3] Dan Eggen. 2007. "Court Will Oversee Wiretapping Program: Change Does Not Settle Qualms about Privacy." *The Washington Post*, January 18. A01.

[4] *Ibid*.

CHAPTER ONE: DEFINING A NEW KIND OF SEARCH

Before examining the present day Foreign Intelligence Surveillance Court and the NSA Terrorist Surveillance Program an extensive examination into the history of electronic surveillance jurisprudence is necessary to establish how these two entities relate to the Fourth Amendment. Practically parallel to the advent of a system of electronic communication, electronic surveillance has been a tool of the executive since the late 19th century. This tool was first used in a national security setting in instances where the Union Army intercepted Confederate telegraphs.[5] As communication technology evolved, so did the ability to intercept communication, yet, by the early 1900s, there was no legal standard established on the subject of electronic surveillance. The Justice Department reports that the first time any Attorney General considered wiretapping for either law enforcement or intelligence purposes was in 1924. Attorney General Harlan Fiske Stone prohibited the use of wiretapping on ethical bounds and law enforcement officers in the Bureau of Investigation (later the Federal Bureau of Investigation) were restricted from using wiretaps for any purpose.[6]

This decision, however, was not a legal one and remained an internal Justice Department guideline. Thus it did not prevent other Cabinet departments from engaging

---

[5] *Berger v. New York.* 388 U.S. 41 (1967).

[6] "Church Committee Report." U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans.* 94th Congress. 1st Session. April 23, 1976.

in wiretapping. This included the Department of Treasury, which at that time was actively investigating violators of the National Prohibition Act. The Bureau of Prohibitions—then a part of Treasury—was the lead entity in arresting bootleggers and did not shy away from the use of electronic surveillance, whether ethical or not. [7] One bootlegger who was subject to such surveillance was a man by the name of Roy Olmstead.

In *Olmstead v. United States*, the Supreme Court issued its first ruling on how electronic surveillance relates to the rights established by the Fourth Amendment. The case began with the arrest of Roy Olmstead and eleven of his conspirators. Olmstead had managed a bootlegging operation within the state of Washington and, in the course of their investigation, law enforcement officers—without entering the building—wiretapped Olmstead's office. Over the course of many months the officers obtained the information needed to arrest Olmstead and this information was used as evidence to convict him. Olmstead appealed his conviction, asserting that his Fourth and Fifth Amendment rights had been violated.[8]

The Court issued its ruling on June 4, 1928. In it Chief Justice William Howard Taft argues that Olmstead's rights were not violated due to the conduct of his conversation and the nature of the process of electronic surveillance. Justice Taft first asserts that "there is no room in the present case for applying the Fifth Amendment, unless the Fourth Amendment was first violated," because Olmstead was not compelled to communicate with his telephone by law enforcement officers. Therefore, Justice Taft

[7] "Church Committee Report."

[8] *Olmstead v. United States*. 279 U.S. 849 (1929).

continues, “consideration must be confined to the Fourth Amendment.”[9] In considering the Fourth Amendment, the Court found that wiretapping did not constitute a search as defined by the Amendment. The Court frames its justification with an examination of cases where searches were physically conducted and then compares them with the Olmstead case where there is “testimony only of voluntary conversations secretly overheard.”[10] The Court did recognize that, in order to consider wiretapping a search, the legal definition of the phrase “search and seizure” would have to evolve with the advances of modern technology. But Chief Justice Taft—with four other justices concurring—was not ready to make this leap. Since there was no physical invasion of “tangible material effects,”[11] the Court did not consider wiretapping to be a Fourth Amendment search.

With four justices dissenting, this opinion, while a majority, was not strongly supported. This not only indicates that *Olmstead* was a narrow ruling, but that, with four justices behind it, the dissenting opinions could eventually evolve into a new type of Fourth Amendment search. Justice Louis D. Brandeis, as one of these justices, “entered a powerful dissent.”[12] He argues that the Fourth Amendment has never had “unduly literal construction”[13] placed upon it. Furthermore, he argues—with the other dissenting justices echoing his call—that the Constitution must evolve with a changing society and that

---

[9] *Ibid.*

[10] *Ibid.*

[11] *Ibid.*

[12] Erin L Brown. “ECHELON: The National Security Agency's Compliance with Applicable Legal Guidelines in Light of the Need for Tighter National Security.” *CommLaw Conspectus*. 2003. 1 CommLaw Conspectus 185.

[13] *Olmstead v. United States.* Brandeis dissent.

evolution must include changes in technology. [14] If technology allows for government to circumvent the literal interpretation of the Constitution through electronic surveillance, then, Justice Brandeis argues, interpretation of the Constitution should uphold the context of the Fourteenth Amendment. Over time, society would continue to evolve, and as it did, the legal arena of electronic surveillance would eventually reform to Justice Brandeis's standards.

In the aftermath of *Olmstead*, the use of information obtained by electronic surveillance in court without a warrant was constitutionally permissive. Even so, state and federal investigations only made sporadic use of this power. For example, Congress passed the Federal Communications Act in 1934 which prohibited wiretapping and, although it was interpreted to allow for some use by federal agents, the Justice Department still considered the practice unethical.[15] With the advent of World War II, however, the use of electronic surveillance within the United States for national security purposes grew and "did not wane with the end of the war."[16]

By the 1950s the Federal Bureau of Investigation had grown considerably due to its importance in national security intelligence during World War II. The Bureau's development as an entity eventually led to its evolution into an "autonomous agency, independent of both the president and attorney general."[17] It was in this era when the FBI's wiretapping practices expanded as the Justice Department now concluded that the

---

[14] Brown, "ECHELON."

[15] "Church Committee Report."

[16] Robert N Davis. "Striking the Balance: National Security vs. Civil Liberties." *Brooklyn Journal of International Law*. 2003. 29 Brooklyn J. Int'l L. 175.

[17] Athan Theoharis. "FBI Wiretapping: A Case Study of Bureaucratic Autonomy." *Political Science Quarterly.* Vol. 107. No 1. (Spring 1992). Pg 104.

Federal Communications Act "did not apply to federal agents."[18] The use of wiretaps increased dramatically and the FBI began to use this surveillance for investigatory, national security and even political purposes.[19]

With electronic surveillance becoming a greater tool in law enforcement, the constitutionality of the practice of wiretapping once again came before the Supreme Court. In 1961 the Supreme Court heard the case *Silverman v. United States* and ruled that when federal agents physically intrude on a person's home to record conversations, they violate the Fourth Amendment.[20] Six years later the case *Berger v. New York* (1967) reached the Court and the justices' interpretation of electronic surveillance took a large step towards Justice Brandeis's view of evolving with society. The Court examined a bribery case where state law enforcement officers obtained judicial approval for a specific form of electronic surveillance known as "bugging." This instance did not involve the wiretapping of a phone line but instead the eavesdropping of a conversation through electronic means. The Court ruled that this instance—while it did have judicial approval—still failed to meet the Fourth Amendment's probable cause standard.[21] Unlike any case before it, in *Berger* the Court ruled that the Fourth Amendment must apply to instances of electronic surveillance because the recorded conversations used in the conviction was a search and seizure as defined by the Fourth Amendment.

Six months later, the final case that brought an end to the Olmstead precedent finally applied this justification to the use of wiretapping within law enforcement

---

[18] *Ibid.*

[19] *Ibid* 105.

[20] *Silverman v. United States.* 365 U.S. 505 (1961).

[21] *Berger v. New York*. 388 U.S. 41 (1967).

investigations. In *Katz v. United States* (1967), the Supreme Court examined a case where the defendant's phone conversation in a public telephone booth was wiretapped and the recording was used to convict him at trial. While the defendant and the government founded their arguments on whether public property was constitutionally protected, the Court took on the issue from a different angle. The Court asserts that "the Fourth Amendment protects people, not places" and thus the issue of constitutionality rests on the concept of privacy and not on the physical location of the defendant. The Court begins its ruling by clarifying that the Fourth Amendment "cannot be translated into a general constitutional 'right to privacy'" but instead protects individuals' privacy against certain types of governmental intrusion.[22] When examining the *Katz* case, the Court held that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[23] Any conversation that an individual seeks to keep private is constitutionally protected and, by recording these conversations, the government performs a search and seizure as defined by the Fourth Amendment.

The question of when one's communication is deemed private and thus falls under the protection of the Fourth Amendment is outlined in Justice Harlan's concurring opinion. This concurrence "provided an important test for a reasonable expectation of privacy in regard to Fourth Amendment protections" which has "remained in effect to this day."[24] Justice Harlan's test broke the issue of privacy into two parts: first, the individual must have demonstrated an actual expectation of privacy; second, this

---

[22] *Katz v. United States.* 389 U.S. 347, 358 (1967).

[23] *Ibid.*

[24] Brown, "ECHELON."

expectation must be one that society is prepared to recognize as reasonable.[25] This reasonableness standard in Justice Harlan's test opens the door to the reality that "the legitimate needs of law enforcement may demand specific exceptions" to normal Fourth Amendment warrants.[26]

This need for exceptions to the general warrant rule was recognized in Katz's majority opinion, with particular emphasis on national security. Footnote 23 of the Court's ruling specifically states, "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."[27] Clearly, the Court left open the question of whether or not electronic surveillance of national security issues required judicial approval. There was even disagreement among the members as to how national security issues should be handled. In his concurring opinion, Justice White elaborates on the need for a national security exception. He contends that the President and the Attorney General should have sole discretion when deciding what constitutes a national security matter. Justice Douglas attacks this view, however, stating that Justice White's interpretation of footnote 23 would give an "unwarranted green light for the Executive Branch" to conduct any electronic surveillance under the guise of national security.[28]

Regardless of the ambiguity found in Justices White and Douglas' dicta on the national security exception, the Katz opinion became the bedrock of electronic surveillance jurisprudence. Congress quickly enacted legislation to establish a process for

---

[25] *Katz v. United States.* Justice Harlan's concurrence.

[26] *Ibid.*

[27] *Katz v. United States.*

[28] *Katz v. United States.* Justice Douglas's concurrence.

law enforcement to obtain warrants for electronic surveillance that abided by the constitutional requirements prevalent in the Fourth Amendment. The Omnibus Crime Control and Safe Streets Act of 1968 defined the bureaucratic procedures to protect the constitutional rights guaranteed to citizens in *Katz*. The executive's authority to conduct electronic surveillance in matters of national security, however, continued unchecked as the act "expressly indicated that it was not intended to interfere with the executive authority of the President" when related to national security.[29] Therefore, when it came to instances of national security, the executive remained immune from the procedural restrictions of judicial scrutiny.

[29] Davis. "Striking the Balance."

CHAPTER TWO: EXPLOITING NATIONAL SECURITY

This avenue for wiretapping without judicial and legislative oversight would not remain open for long, however, as certain events caused both the Supreme Court and Congress to begin to examine this issue more stringently. The first instance of applying Forth Amendment standards to wiretapping for national security reasons came in the case *United States v. United States District Court for the Eastern District of Michigan.* It became known among legal scholars as the *Keith* case because the government filed a writ of mandamus challenging the decision by then District Judge Damon J. Keith.[30] Judge Keith had ordered the government to disclose the transcripts of warrantless electronic surveillance information related to national security. The case involved three individuals indicted for conspiracy to destroy Government property. One of the defendants was also charged with the dynamite bombing of a Central Intelligence Agency office building. This defendant moved to have the government disclose the recorded conversations and also moved to hold hearings to determine whether these recordings "tainted" the evidence found in the indictment.[31] This was the first time that the national security exception to the Fourth Amendment procedural protections had reached the Supreme Court. In essence, the Court was asked to take up the debate that Justices White and Douglas had engaged in with their concurrences in *Katz*.

---

[30] John Cary Sims. "What NSA Is Doing ... and Why It's Illegal." *Hastings Constitutional Law Quarterly*. Winter / Spring, 2006. 33 Hastings Const. L.Q. 105.

[31] *United States v. United States District Court for the Eastern District of Michigan et al*. 407 U.S. 297 (1972).

The Court, in its opinion, held that footnote 23 of *Katz* and the national security exceptions in Title III were not grounds for complete disregard for Fourth Amendment protections. The Court found that "official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech."[32] Such a risk, the Court argues, does "not justify departure in this case from the customary Fourth Amendment requirement of judicial approval prior to initiation of a search or surveillance."[33] Clearly, with the ruling in the *Keith* case, the national security exception in electronic surveillance practices shrunk significantly.

This exception, however, was not completely eliminated. The Court had ruled within the context of the *Keith* case, only in reference to situations where *domestic* organizations threaten national security. The Court was quick to point out the limits this ruling had when applied to electronic surveillance levied against *foreign* threats. The ruling makes sure to note that the Court is not addressing the issue "with respect to activities of foreign powers or their agents."[34] The Court further argues "that warrantless surveillance, though impermissible in domestic security cases, may be constitutional where foreign powers are involved."[35] Once again the Court extended the application of Fourth Amendment protections in the realm of electronic surveillance law, yet left open a door for the executive to continue some form of surveillance free from judicial scrutiny. In fact, for many years after the Keith case, the attorney general was allowed to "authorize surveillance of foreign powers and agents of foreign powers without any court

[32] *Ibid.*

[33] *Ibid.*

[34] *Ibid.*

[35] *Ibid.*

review."[36] Congress, however, eventually discovered this exception also led to many forms of executive abuse. This led to a political atmosphere that was finally ready for establishing Article III checks on all forms of electronic surveillance.

In response to this executive branch abuse Congress, in 1976, began to investigate the possibility of executive misuse of electronic surveillance by creating the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, referred to as the Church Committee after Senator Frank Church. On April 23, 1976, the Church Committee issued a report which, in part, outlined various instances of executive misconduct within the realm of electronic surveillance practices. The committee noted that after the ruling in the Keith case restricting most forms of warrantless electronic surveillance, "all existing warrantless electronic surveillances were directed against foreigners."[37] This demonstrates that the executive branch had now ceased all warrantless surveillance previously allowed before the ruling in Keith. This did not, however, prove that there was no abuse of electronic surveillance policy. The committee also noted that the proportion of foreign targets had grown significantly after the Keith ruling,[38] indicating that the executive was utilizing the foreign powers exception in order to circumvent judicial scrutiny.

This abuse was not limited to one party or one president. The committee offered examples of multiple administrations improperly applying the foreign powers exception. Attorney General Robert F. Kennedy authorized the surveillance of Congressmen in their

---

[36] *The 9/11 Commission Report*. The National Commission on Terrorist Attacks Upon the United States. July 22, 2004. Public Law 107-306. http://www.9-11commission.gov/report/index.htm. Pg 78.

[37] "Church Committee Report."

[38] *Ibid*.

negotiations with foreign officials on sugar quota proposals, an action clearly not related to the protection of national security. Kennedy also authorized wiretaps on the residence and office of Dr. Martin Luther King, Jr. merely on the bases that two of his associates may have been associated with the Communist Party.[39] The Kennedy Administration was not the only one to engage in questionable electronic surveillance policy. President Lyndon Johnson personally told the FBI to inform him on foreign officials' contact with Congressmen. This directly resulted in the electronic surveillance "of each Senator, Representative, or staff member who communicated with selected foreign establishments."[40] One documented incident also showed that, at the request of President Johnson, the FBI "instituted an electronic surveillance of a foreign target for the purpose of intercepting telephone conversations of a particular American citizen."[41]

These practices continued under President Richard Nixon; the administration informed the FBI that they "wanted any information … relating to contacts between [certain foreign officials] and Members of Congress and its staff."[42] Furthermore, the Nixon administration used these exceptions to justify "his departures from electronic surveillance law. In the wake of these discoveries, Congress determined that additional statutory protections were needed to close the loopholes in Title III."[43]

---

[39] *Ibid*.

[40] *Ibid*.

[41] *Ibid*.

[42] *Ibid*.

[43] Grayson A. Hoffman. "Litigating Terrorism: The New FISA Regime, the Wall, and the Fourth Amendment." *American Criminal Law Review*. Fall, 2003. 40 Am. Crim. L. Rev. 1655.

Clearly, these violations show that misuse of executive electronic surveillance was widespread throughout the 1960s and 1970s. This misconduct continued in every administration, regardless of party affiliation. Not only was the Fourth Amendment privacy of multiple U.S. persons violated by the executive's actions, but "moreover, the use of warrantless electronic surveillance against… attorneys, Congressmen and Congressional staff members, and journalists, has revealed an insensitivity to the values inherent in the Sixth Amendment and the doctrines of 'separation of powers' and 'freedom of the press'."[44] The fact that these actions were not well-intended attempts at protecting national security but instead complex conspiracies to spy on political opponents shows that any form of electronic surveillance without judicial authorization undoubtedly has direct harm on the American system of democracy.

[44] "Church Committee Report."

CHAPTER THREE: CHECKING FOREIGN INTELLIGENCE

Given the prevalent abuse of electronic surveillance by the executive branch, the Church Committee supported a piece of legislation which had already been introduced into Congress.[45] This law would designate federal judges to find probable cause that a suspect is a foreign power or agent of a foreign power before electronic surveillance could be initiated. The Church Committee considered this solution to be a "significant step towards effective regulation of FBI electronic surveillance."[46]

Based upon this Church Committee recommendation, Congress blocked the final avenue for warrantless electronic surveillance. The Foreign Intelligence Surveillance Act was passed in 1978. "This law regulated intelligence collection directed at foreign powers and agents of foreign powers in the United States" and brought the only remaining avenue for warrantless electronic surveillance under Article III jurisdiction.[47] Some legal scholars contend that "FISA represents an effort by the political branches to promote judicial involvement in fighting threats to the national security."[48] While it is true that FISA includes the judiciary in the process of protecting national security, it is important to recognize that the true foundation of FISA "was a reaction to executive branch abuses

---

[45] "Church Committee Report."

[46] *Ibid*.

[47] *The 9/11 Commission Report*. Pg 78.

[48] John C. Yoo. "Judicial Review and the War on Terrorism." *The George Washington Law Review*. December, 2003. 72 Geo. Wash. L. Rev. 427.

of civil liberties."[49] Congress recognized that a response to the multiple Fourth Amendment violations found by the Church Committee was needed; this new legislation—while including the judiciary into the realm of national security—was established solely to provide an Article III check on the executive's wiretapping authority.

The Foreign Intelligence Surveillance Act took specific steps to provide a check on the executive's electronic surveillance in matters of foreign affairs and eliminated the practice of electronic surveillance without judicial approval. First the Act established a judicial entity to oversee all electronic surveillance not covered under Title III protections. Thus the area of electronic surveillance not covered by the *Keith* case—foreign powers or agents of foreign powers—were brought under the jurisdiction of the Foreign Intelligence Surveillance Court. This Court consists of judges from various federal district courts publicly appointed by the Chief Justice of the Supreme Court to serve nonrenewable seven year terms.[50]

In order to engage in electronic surveillance, the government must receive approval from this Court by meeting specific standards laid out in the Act. The government must demonstrate "probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power."[51] The statute further defines the terms "foreign power" and "agent of a foreign power," relating them to espionage and international terrorism. FISA also establishes notice and suppression

---

[49] Davis. "Striking the Balance."

[50] Rebecca A. Copeland. "War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America." *Texas Tech Law Review.* 35 Tex. Tech L. Rev. 1. (2004).

[51] 50 U.S.C. 1805 (18) (I).

requirements different than traditional Title III requirements and dictated that the foreign intelligence must be the primary purpose of the surveillance.[52]

With the passage of FISA, Congress restricted the final avenue open to the executive for obtaining domestic electronic surveillance without a court order. This new system for electronic surveillance of foreign powers then began to evolve within the bureaucratic structure. Throughout the 1980s and 1990s the Department of Justice created "procedures limiting contact between foreign intelligence agents in the FBI and federal prosecutors. Those procedures … produced what the public came to call 'the wall.'"[53] This system was created to comply with the "primary purpose" standard set out in FISA. The Department of Justice concluded that if foreign intelligence agents who used FISA proceeding in gathering intelligence were not able to collaborate with criminal prosecutors then those agents would always meet the primary purpose standard. Yet, as it was only Justice Department policy and not a statutory mandate, this "wall" separating shared intelligence between foreign intelligence and law enforcement agents was a bureaucratic construction and, while recognized as acceptable procedure by some lower courts, was never constitutionally mandated by Congress or the judiciary.

This "wall" first formed by the executive bureaucracy stemmed from a series of misinterpretations of the FISA statute and subsequent policies. These misinterpretations lead to serious problems of intelligence gathering within the intelligence community. Congress had created the "primary purpose" standard in order to prevent authorities from

---

[52] Hoffman, "Litigating Terrorism."

[53] Richard Henry Seamon and William Dylan Gardner. "The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement." Harvard Journal of Law & Public Policy. 28 Harv. J.L. & Pub. Pol'y 319. (Spring, 2005).

using FISA to "circumvent traditional criminal warrant requirements."[54] Yet the Department of Justice took a stringent interpretation of FISA; federal prosecutors were not allowed to control or direct the collection of FISA investigations and the FBI—not federal prosecutors—had sole discretion in what information the Justice Department could view. In 1995, further policies established by then Attorney General Janet Reno again "were almost immediately misunderstood and misapplied."[55] First, although the new polices did not require it, the DOJ's Office of Intelligence Policy Review became the sole gatekeeper for passing information through Justice Department channels. OIPR and FBI leadership pressured the agents into building further barriers between agents working on intelligence gathering and agents working on criminal investigations. These restrictions lead to the practice of restricting information from criminal investigators even when no FISA procedures had been used.[56]

This divide in the sharing of information between intelligence agents and law enforcement officials continued to be the norm until the entire system of foreign intelligence gathering was reviewed in the wake of the tragic events of September 11th. In response to the "pervasive problems"[57] evident in the intelligence community that led up to the attacks in New York City and Washington D.C., Congress passed the controversial USA PATRIOT Act of 2001. The many changes that the PATRIOT Act incorporated included the breaking down of the bureaucratic wall that separated the sharing of intelligence. In relation to FISA, the PATRIOT Act attempted to break down this wall by

[54] *The 9/11 Commission Report*. Pg 78.

[55] *Ibid.*

[56] *Ibid*. Pg 79.

[57] *Ibid.* Pg xvi.

amending FISA's "primary purpose" standard to a "significant purpose" standard. This change was the result of a compromise between those at Justice who wanted the "primary purpose" standard revoked and those who supported the original form of the FISA procedure.[58] This compromise allowed for shared information between intelligence officers and law enforcement agents within their respective investigations and also allowed for the use of FISA surveillance in criminal proceedings.

Reconsideration of the Federal Intelligence Surveillance Act was challenged within the federal courts, although subsequent rulings supported to its constitutionality. The first notable case took place in 1984, before the amendments of the PATRIOT Act. In *United States v. Duggan*, the defendant—a member of the Provisional Irish Republican Army—was convicted on charges of transporting explosives via interstate commerce that would be used to kill, injure or intimidate individuals. A FISA Court order was issued to allow electronic surveillance of the individual and his accomplices. The defendant challenged his conviction, arguing first that FISA's definition of foreign power is too broad and thus deprives him due process of the law, and that it violates the probable cause standard within the Fourth Amendment.[59] The U.S. Court of Appeals for the Second Circuit ruled that the definition was not too broad and that the probable cause standard in FISA is constitutional because, as the surveillance falls under the umbrella of national security, an adequate balance between a legitimate need of the government and the protected rights of citizens was struck within FISA's language.[60]

---

[58] Seamon and Gardner. "The Patriot Act and the Wall."

[59] *United States v. Duggan.* 743 F.2d 59 (1984).

[60] *Ibid*.

The second case to be examined occurred after the amendments of the PATRIOT Act and dealt with the Act's changes to the original FISA "primary purpose" standard. This case took place within FISA's judicial structure as it was the first published opinion of the FISA Court of Review. This court was established in the original statute as the government's only means of appeal when a FISA Court order request is denied. In this case, the original FISA Trial Court judge denied a request by the government and stated that the "primary purpose" test still had to be met within the FISA statute. The FISA Court of Review, in its first ever issued opinion, *In re Sealed*, ruled for the government, stating that the PATRIOT Act had lowered the test to a "significant purpose" standard. The FISA Court of Review also rejected the argument of amici curiae that it was constitutionally necessary to keep intelligence investigations separate from law enforcement investigations.[61] The Court of Review considered the wall constructed between federal intelligence agents and law enforcement agents as a bureaucratic misinterpretation of FISA. The Court held that the Fourth Amendment was not violated with the prosecution of foreign intelligence crimes.[62]

[61] *In re Sealed.* 310 F.3d 717.

[62] Davis. "Striking the Balance."

CHAPTER FOUR: DEFENDING THE FISA COURT

With the passage of FISA and the subsequent appellate court decisions defending its constitutionality, Congress and the judiciary had sealed the last remaining avenue for the executive to engage in electronic surveillance without a court order. However, with the development of current events, debate has arisen as to whether or not electronic surveillance laws and practices adequately protect citizens' Fourth Amendment rights. Arguments are levied on both sides; some defend recent practices, such as the NSA's controversial Terrorist Surveillance Program, that go outside the bounds of FISA and Title III law, while other legal scholars attack the post PATRIOT Act FISA procedures as infringing on citizens' constitutional rights. Yet with a careful examination of the jurisprudence surrounding recent electronic surveillance laws, an adequate balance can be found. This balance of national security and individual, constitutional rights is achieved when the only means of domestic electronic surveillance are Title III warrants and post PATRIOT Act FISA Court orders. Any programs, such as the NSA's Terrorist Surveillance Program, which do not conform to the established Title III or FISA procedures, unduly infringe on the civil liberties of United States citizens and are therefore outside the grounds of the Constitution.

Before this paper continues in its argument that, currently, the executive branch's Terrorist Surveillance Program is unconstitutional, it must be conceded that the post PATRIOT Act FISA Court is not an acceptable institution to some legal scholars with regards to the Fourth Amendment. Thus, in order to argue that a constitutional balance of

civil liberties and national security can be reached, this paper must accomplish three tasks: first it must mount an adequate defense of the FISA Court; then it must show that the Terrorist Surveillance Program intruded on Fourth Amendment protections by violating important constitutional checks and balances; finally, solutions must be examined which would make sure that future abuses of executive power in the realm of electronic surveillance is minimized.

Legal scholars tend to have four main contentions with the constitutionality of the FISA Court: first, many assert that the lack of public proceedings and notification requirements are contrary to the Constitution; second, many argue that the different probable cause standard is unreasonable within the context of the Fourth Amendment; third, that the "wall" restricted shared intelligence is necessary to protect civil rights; finally, many legal scholars argue that FISA Court orders allow for abuse of executive power. This paper will examine all four main arguments and conclude that FISA Court orders—while they do use standards different than Title III warrants—are still reasonable within the Fourth Amendment.

Many organizations assert that FISA proceedings are secret and thus contrary to the established system of open government. They claim that, in a democracy, judicial procedures must remain within the public's knowledge to insure the government is not intruding on constitutional rights.[63] While public proceedings are an important part of adhering to an open and legitimate form of government, there are many instances where

---

[63] Jim Dempsey, Alan Davidson and Jerry Berman. "DOJ Proposes Further Surveillance Expansion Changes to Intelligence Authorization Would Again Increase FISA Eavesdropping." Center for Democracy and Technology. CDT Preliminary Analysis. November 30, 2001. http://www.cdt.org/security/011130cdt.shtml. and;

"ACLU Applauds House Introduction of FISA Oversight Bill." American Civil Liberties Union. *Safe and Free*. http://www.aclu.org/safefree/general/16872 prs20030611.html. June 11, 2003.

public access is restricted for reasons of national security. Many aspects of society are classified or restricted from public access; from certain bureaucratic regulatory hearings to internal documents and classified intelligence, there are undoubtedly instances where information cannot be publicly available. Yet national security or public interest claims cannot counter all assertions of the need for open access to government. In fact, when this discussion enters the realm of the Fourth Amendment, legal precedents often requires public proceedings and notification requirements. Electronic surveillance is unique in regards to other Fourth Amendment searches however, as the target of the surveillance cannot be notified of the search until it is completed, or else the purpose of the surveillance is mute. Therefore, when it comes to electronic surveillance, the Court has consistently held that there is a legitimate government interest in restricting the public's access to certain proceedings and delaying the notification requirements.[64] This concept of weighing government's interest against the requirements in the Fourth Amendment continues to hold its balance when examining FISA Court orders. The differences between Title III electronic surveillance warrants and FISA Court orders are minimal when it comes to public proceedings. Both proceedings are *in camera* and *ex parte*. Title III procedures are sealed while FISA orders are classified. Thus both processes are restricted from public access and both essentially have the same effect: because of the inherent secrecy involved in electronic surveillance the government has a legitimate interest in restricted public access.

There is one significant aspect of FISA Court orders that is not parallel to the Title III procedures when it comes to notification. In the Title III procedure "all targets

[64] *Katz v. United States.*

must receive notice … that they were the target of an electronic investigation. FISA only requires notice to the target when the government intends to use the information as evidence in trial against them."[65] When analyzing the differences in these procedures, two different balancing tests must be applied. First, in Title III warrants, the privacy rights of a citizen to know when he or she has been the target of a search are balanced against the government's compelling interest in enforcing the law. Therefore, after the search is completed, the government either has the choice to prosecute, and must then disclose the evidence collected in the search, or must decide not to pursue charges, in which case the government's compelling interest to keep the citizen ignorant to the search is mute. It follows that the only constitutionally acceptable avenue is notification. In FISA Court orders, the standard shifts weight. The government—when it is opting not to engage in a criminal prosecution—has a compelling interest to keep the search secret. There is a fundamentally different purpose for FISA Court orders; whether criminal prosecutions are involved or not, FISA orders are enacted to prevent threats posed to national security. This fact, when balanced against a citizen's right to be notified that a search has taken place, is compelling enough for the information to remain secret.

Furthermore, while FISA Court orders do differ in the aspect of notification, this standard is only different when the government is *not* planning to prosecute the subject of the FISA surveillance. The government's interest in protecting national security in relation to the notification of electronic surveillance against foreign powers only outweighs the rights of the agents of foreign powers when collecting intelligence. When the government seeks to use electronic surveillance in the arena of law enforcement and

[65] Hoffman, "Litigating Terrorism."

seeks to initiate any criminal prosecution, the rights of the targeted foreign power then trump the government's need for secrecy. The government, if it desires to use FISA Court information in a criminal procedure, must allow the defendant, and the defendant's attorneys, access to the information.[66] Clearly, when examining FISA procedures through this balancing test, FISA Court orders meet the reasonableness clause of the Fourth Amendment.

Public procedures and notification requirements are not the only contention with the FISA Court. Some scholars also argue that the lessened probable cause standard used to issue FISA Court orders violates the Fourth Amendment.[67] First, however, it is important to note that case law is ambiguous as to whether or not FISA Court orders are "warrants" as defined by the Fourth Amendment. Although the government argued that they were in *In re Sealed*, the Court of Review stopped short of addressing the question. The Court did, however, review the question of the reasonableness of FISA Court orders and found them to meet the standards set by the Fourth Amendment. This conclusion is not outside precedent as the Supreme Court has upheld many instances of reasonable exceptions to the warrants clause.

In order to meet the Fourth Amendment reasonableness standard both Title III warrants and FISA Court orders have different probable cause standards. Title III warrants require the government to show probable cause that a crime was committed or is about to be committed. This is because the purpose of a Title III warrant is solely based on enforcing the law. Thus, a person's right to remain secure from an unreasonable search is weighed against the government's compelling interest to enforce the law. FISA

---

[66] Davis. "Striking the Balance."

[67] *In re Sealed.*

Court orders, once again, require a different balance. A person's right to remain secure from an unreasonable search is now weighed against the government's compelling interest to protect national security. To examine this balance the purpose of Title III warrants verse the purpose of FISA Court orders must again be examined. Title III warrants are issued to collect evidence that a crime has been committed in order to prosecute that crime. When working against terrorists, however, the government must act to *prevent* terrorist actions. As one legal scholar states, "Title III … was crafted to punish and deter normal crimes" whereas "FISA procedures … were specifically created to prevents such crimes *before* they occur."[68] This need to prevent terrorist activities shows the government's compelling interest to have a lessened probable cause standard, as demonstrated in the *Duggan* case. Furthermore, it must be understood that this standard only applies to a very narrow portion of the population. The government must demonstrate probable cause that the target is a foreign power or an agent of a foreign power. Also, the Foreign Intelligence Surveillance Act's definition of an agent of a foreign power is "rooted in criminal conduct,"[69] such as terrorism or espionage. Thus the probable cause standard is similar to the Title III standard because both are based off criminal actions. This standard is further narrowed when a citizen is targeted; the government cannot base their evidence of probable cause solely on the target's First Amendment actions.[70]

---

[68] Hoffman, "Litigating Terrorism."

[69] *Ibid*.

[70] *Ibid*.

Some legal scholars accept the fact that notification and probable cause standards differ when the government's interests in the surveillance change yet still assert the current application of FISA is unconstitutional. They argue that the USA PATRIOT Act altered the "primary purpose" standard set in the original version of FISA and thus violated the wall between intelligence sharing and law enforcement.[71] These scholars contend that that wall is a constitutional necessity rather than a bureaucratic construction.[72] This contention, however, is contrary to the previous examination of the jurisprudence surrounding the PATRIOT Act's amendments to FISA. In *In re Sealed*, the FISA Court of Review held that the primary purpose standard was not constitutionally binding.[73] The government's compelling interest in protecting national security still allows for electronic surveillance of foreign powers when the government demonstrates that a significant purpose of the surveillance is for foreign intelligence. Furthermore, many legal scholars hold that the original interpretation of FISA by the Justice Department that a wall should be constructed between intelligence agents and law enforcement officers "has never had a statutory foundation and still lacks one."[74] The only contradictory precedent to this anaylisis is the pre-FISA case *United States v. Truong* which first coined the "primary purpose" standard. Yet, because this case was "a pre-FISA case that never analyzed the Fourth Amendment implications of a significant

---

[71] Copeland, "War on Terrorism or War on Constitutional Rights?"

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

[73] *In re Sealed.*

[74] Seamon and Gardner. "The Patriot Act and the Wall."

purpose test," the Court of Review found it inapplicable.[75] "In other words, criminal investigation can be used as the *primary* tool to fight foreign-based threats such as terrorism or counterintelligence. Because Truong neglected this glaring reality, the court concluded, *Troung* was neither binding nor persuasive in connection with FISA's new significant purpose test."[76] Clearly, neither the "significant purpose" nor the "primary purpose" tests erected a wall separating foreign intelligence gathering and prosecutorial surveillance.

The FISA Court of Review did establish a standard to restrict the government's use of FISA orders that was mandated by the Fourth Amendment. The government must "draw a line between 'foreign intelligence crimes' and 'non-foreign intelligence crimes'" in order to abide by FISA and the Fourth Amendment.[77] While statutory law is ambiguous in this regard, it is a necessary component of FISA procedure. Finally, the argument that constitutionality rests on whether surveillance is conducted for foreign intelligence purposes or law enforcement purposes lacks logical foundation within the Fourth Amendment. The Fourth Amendment protects citizens' right to privacy when the government conducts an unreasonable search and seizure. Therefore, reasonableness is dependent on the *search,* not on the use of the information obtained in the search. For example, if the government were to wiretap an individual without any court approval, and it was clearly not within any exceptions to court approval, then the unreasonable search of the individual—and thus the violation of the Fourth Amendment—has already taken

---

[75] Hoffman, "Litigating Terrorism."

[76] *Ibid.*

[77] Seamon and Gardner. "The Patriot Act and the Wall."

place, regardless of whether the government intends to use the information in trial. Whether or not the information is to be used in a court proceeding is inconsequential; the government need only show a significant purpose of foreign intelligence and the probable cause to believe the target is a foreign power in order to use FISA authorized electronic surveillance.

Clearly, the standards applied to FISA Court orders are reasonable when viewed in their narrow context. The government can only use the lower standards in FISA when probable cause that the target is a foreign power or an agent of a foreign power exists and "generally speaking, FISA does not authorize secret surveillance of average American citizens."[78] Courts have held that these terms are not broad, and are in fact clearly defined in the FISA statute.[79] Some legal scholars do contend, however, that FISA procedures still allow for misuse by the executive branch.[80] Clearly, this view is unfounded, because FISA uses the same check on executive power that is found in Title III warrants. The safeguards that protect statutory violations of civil liberties are different in Title III and FISA procedures, yet the safeguard that exists to protect against executive misuse of electronic surveillance is the same in both procedures: judicial approval. Both FISA orders and Title III warrants require the government to obtain approval from an independent judicial authority. As with Title III procedures, if an adequate judicial check on every one of the executive's request to initiate electronic surveillance, then instances of misuse by the government can be significantly minimized.

---

[78] Copeland, "War on Terrorism or War on Constitutional Rights?"

[79] *United States v. Duggan*. 743 F.2d 59 (1984).

[80] Dowley, "Government Surveillance Powers."

CHAPTER FIVE: BREAKING WITH FISA LAW

Unfortunately the statutory status quo previously analyzed is not the de facto situation that has occurred after September 11th. This paper will continue by analyzing the Terrorist Surveillance Program and how it contrasts with decades of electronic surveillance jurisprudence. Next it will be argued that if the administration was granted blanket authorization to continue the TSP from a FISA Court judge, then the administration is still acting outside the scope of the law. Finally, a number of recommendations will be presented that—if implemented—will help to return, and to keep, the actions of the executive branch back within legal realm of electronic surveillance policy.

First publicly reported in the *New York Times*, in 2002 the President signed an order secretly authorizing the National Security Agency to use electronic surveillance to spy on individuals within the United States without first seeking approval from the Foreign Intelligence Surveillance Court.[81] This program, though animatedly defended by the Bush Administration, is criticized by many legal scholars as violating both statutory and constitutional law. The Terrorist Surveillance Program continued despite criticism, and not until January of 2007 did the administration announced TSP would now be under the authority of the FISA Court. This recent shift in policy does not mean the program is now within the boundaries of the law, however, as the "precise outlines of and legal

[81] Katherine Wong. "Recent Development: The NSA Terrorist Surveillance Program." *Harvard Journal on Legislation*. Summer, 2006. 43 Harv. J. on Legis. 517. and;

The National Security Agency's Domestic Spying Program. January 9, 2006. Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department Letter of December 22, 2005.

justification for the monitoring remain unclear."[82] While the administration has indicated they plan to brief certain Senate Judiciary members on the changes, the administration has failed to say whether the Terrorist Surveillance Program has been completely eliminated, or whether a single FISA Court judge has given blanket authorization of the program. Recent comments by the President seem to infer the latter: "the FISA court said I did have the authority … it's important that they verify the legality of this program is it means it's going to extend … yesterday was a very important day for the Terrorist Surveillance Program. Nothing has changed in the program except for the court has said … it is a legitimate way to protect the country."[83] Regardless of the ambiguity, it is clear that for over five years the administration circumvented the statutory laws regulating the use of electronic surveillance.

It is clear that the justifications for the administration's use of the TSP do not hold up to thorough examination. Many scholars—as well as current and former government officials—conclude "that the program is illegal."[84] Several also argue that the motives behind the TSP were to "circumvent FISA's court-approval process with respect to electronic surveillance that would be authorized by FISA and, almost certainly, to engage in forms of surveillance that FISA prohibits."[85] It is undoubtedly clear that this program is contrary to federal court precedent because it allows for electronic surveillance on domestic United States soil without judicial approval or any showing of probable cause.

---

[82] Eggen, "Court Will Oversee Wiretapping."

[83] Dan Froomkin. "Bush: No Retreat on Spying." *The Washington Post*. January 19, 2007. www.thewashingtonpost.com.

[84] Wong. "Recent Development."

[85] David Cole and Martin S. Lederman. "The National Security Agency's Domestic Spying Program: Framing the Debate." *Indiana Law Journal*. Fall, 2005. 81 Ind. L.J. 1355.

The administration still defends the legality of the program, however, and believes the program is allowed under the Authorization for Use of Military Force.[86] Congress passed the AUMF just after the September 11th terrorist attacks, authorizing the President "to use all necessary and appropriate force" against "persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2003."[87] This Act, the administration argues, allows for the TSP because warrantless surveillance is included in "all necessary and appropriate force." Furthermore, the administration argues that they are not acting outside of the scope of FISA. They also contend that tacit judicial approval for the TSP is granted through the Supreme Court case *Hamdi v. Rumsfeld.*[88]

A significant number of legal scholars, as well as many government officials, seriously disagreed with the administrations interpretation of the expansion of executive power implied in the AUMF. On January 9, 2006 several of these scholars drafted a letter to the Department of Justice outlining their contentions with the program and arguing that the TSP was in violation of United States statutory and constitutional law.[89] The letter outlined the why the administration's defense of the Terrorist Surveillance Program does not hold up to statutory law and legal precedent surrounding the use of electronic surveillance. They argue that the implication that the AUMF allows for complete warrantless wiretapping on domestic soil "directly contradicts *express* and *specific*

---

[86] Wong. "Recent Development."

[87] Authorization for the Use of Military Force. Senate Joint Resolution 23, House Joint Resolution 64. Congressional Record. Volume 147 (2001).

[88] *The Legal Authority for NSA Surveillance*. December 22, 2005. Department of Justice Letter from Asst. Attorney General William E. Moschella to Congress.

[89] *The National Security Agency's Domestic Spying Program*. Letter from Scholars.

language in" the Foreign Intelligence Surveillance Act.[90] FISA specifically states that it—along with Title III wiretaps—are the "exclusive means by which electronic surveillance … and the interception of domestic wire, oral and electronic communications may be conducted."[91] Clearly, for the administration to believe that the ambiguous language in the AUMF overrides the specific procedures laid out in FISA is completely unreasonable.

Even if Congress intended to repeal FISA with the AUMF, the scholars argue, the evidence of such intent would, by case law precedent, have to be "overwhelming."[92] Citing *Morton v. Mancari* (1974), they argue that, since the two statutes in conflict are not "irreconcilable," the evidence is not considered overwhelming enough for the administration to legally infer the intent of Congress.[93] Clearly, based on precedent, the administration could not legally infer Congress tacitly approved of the implementation of the TSP. Furthermore, the legal scholars point out a serious contradiction in the administration's justification for the program. They first cite that the Attorney General "has admitted that the administration did not seek to amend FISA to authorize the NSA spying program because it was advised that Congress would reject such an amendment."[94] Clearly this is a blatant contradiction to their claims of tacit approval of Congress; if the legislative branch had intended to approve of the Terrorist Surveillance

---

[90] *Ibid.*

[91] 18 U.S.C. 2511 (2) (f).

[92] *The National Security Agency's Domestic Spying Program*. Letter from Scholars.

[93] *Morton v. Mancari.* 417 U.S. 535 (1974).

[94] *Ibid.*

Program in the AUMF, then the administration would not need to fear a possible rejection from Congress.

Lastly, the legal scholars note that the only case law the administration uses to defend the legality of the Terrorist Surveillance Program is the recently decided case *Hamdi v. Rumsfeld*. Yet this case held that, under the AUMF, the administration is only allowed to hold enemy combatants captured on the battlefield, and in fact, it contradicted the administration's assertion that the AUMF allows for domestic use of force. The Court's narrow ruling in this case in no way justified the extension of the executive branch's electronic surveillance powers. It dealt entirely with Congress's intent as it applied to the literal battlefield of a foreign front, "it is another matter entirely to treat unchecked warrantless *domestic* spying as included in that authorization."[95] The Court undoubtedly found that Congress had implied the power for the administration to hold enemy combatants obtained on a foreign battlefield; yet for the administration to view this ruling as an extension of executive electronic surveillance is unfounded.

While these contentions were raised as soon as the TSP was publicly announced, the administration did not change their stringent support of the program until January 2007. As previously examined, the administration did bring the program under the authority of the FISA Court. Yet this move brings new and difficult questions to the table. It is unclear as to whether or not the FISA Court is examining every individual request for surveillance under the TSP or whether the single FISA judge gave the program blanket authorization. If the FISA Court judge did give the program authorization in its entirety, then serious constitutional issues remain. First, a FISA Court

[95] *Ibid.*

judge has no statutory jurisdiction to authorize an entire surveillance program; the Foreign Intelligence Surveillance Act only allows FISA Court judges to rule on individual cases concerning individual targets where the government has probable cause to believe they are agents of a foreign power. From what is known of the Terrorist Surveillance Program, no protections exist to distinguish agents of foreign powers and other U.S. persons. Furthermore, there is no real Article III protection for civil liberties under this situation. Only individual evaluation of each wiretapping application by an Article III judge can protect against Fourth Amendment violations.[96] Clearly, "the terrorist surveillance program directly conflicts with the judicially sanctioned procedure for conducting warrantless electronic surveillance"[97] and violates both statutory and constitutional precedent.

[96] Wong. "Recent Development."

[97] *Ibid.*

CONCLUSION

When analyzing other areas of government where electronic surveillance is used for criminal investigations, it is clear that American society is wary of its extended use. State governments have been quick to limit electronic surveillance by law enforcement. While local legislatures have no jurisdiction over the use of federal wiretaps, most have not significantly altered their own wiretapping laws in the post 9-11 era. While "New York lawmakers broadened their wiretap laws to add terrorist activities to the list of offenses police can investigate with electronic eavesdropping … only one other state—Florida—is considering following New York's lead."[98] Furthermore, many states have also extended the guidelines for their applications for electronic surveillance; some going as far as limiting how many wiretaps are allowed in a given year, while others have even restricted the use of information obtained in wiretaps in criminal court proceedings.[99]

More specifically, there are strong indications that the American public is wary of the current administration's decision to use the Terrorist Surveillance Program to authorize warrantless wiretapping. A Los Angeles Times/Bloomberg Poll conducted in April 2006 found a plurality of those polled considered the TSP an unacceptable way for the federal government to investigate terrorists. A plurality of those polled also believed

---

[98]Kathleen Murphy. "States Go Slow on Wiretap Expansion." *Stateline.org*. Pew Research Center. October 12, 2001. http://www.stateline.org/live/ViewPage.action?siteNodeId=136&languageId=1&contentId=14507.

[99]Jannan Goodwin, Robert D. Boerner and Susan Frederick. "Electronic Surveillance." *Protecting Democracy: States Respond to Terrorism.* National Conference of State Legislatures. http://www.ncsl.org/programs/press/2002/issues/surveillance.htm; and

Kari Berge, ed. "Electronic Surveillance Warrant Procedures." *State Wiretapping Procedure Laws.* National Conference of State Legislatures. http://www.ncsl.org/ programs/lis/CIP/wiretap-proc.htm.

that the U.S. Senate should censure the President because of these actions.[100] This shows that not only do a significant number of legal scholars believe that the Terrorist Surveillance Program is unconstitutional but that the general American public—even in a post 9-11 environment—is wary of the administration's use of warrantless electronic surveillance.

In order for this electronic surveillance system to revert back to the realm of constitutionality, certain solutions must be implemented from policy makers in Washington. Clearly, "the solution should come from legislation."[101] Many legal scholars assert that changes must be made in order to bring the system back under the proper jurisdiction of the FISA Court. First, Congress must pass legislation which specifically denies a single FISA Court judge from giving the TSP—or any similar program—blanket authorization. The jurisdiction of any FISA Court judge should be reemphasized as only dealing with individual requests for targets who the government can demonstrate probable cause that the person is an agent of a foreign power. With such statutory mandates, electronic surveillance policy would then return to the necessary constitutional standard. Next, legislation must address the Terrorist Surveillance Program specifically; it should either eliminate the program in its entirety or mandate that the process be brought under the FISA Court and the procedure meet FISA standards. Next, if Congress deems the National Security Agency needs more flexibility in its actions, legislators should make sure any reforms are constitutional sound. Many legal scholars assert that

---

[100] *Los Angeles Times*. April 8 – April 11, 2006. The Roper Center for Public Opinion Research. The University of Connecticut. iPoll Databank.

[101] Wong. "Recent Development."

changes could be made to expedite the FISA order process.[102] This could include combining requests into one application yet giving FISA Court judges line item veto power within their orders, or Congress could create different probable cause standards which would align with legal precedent but would also give the NSA a different approach to specific national security issues.[103] Lastly, Congress must begin—and continue—rigorous oversight of the executive's use of electronic surveillance programs. The desire to keep information classified and out of Congress's view cannot override Congress's important responsibility to act as a check on executive power. Only with these—or similar—changes to the structure of electronic surveillance policy can the integrity and legality of the system be recognized by the legal community.

Finally, some legal scholars argue that—regardless of the legality of the program—national security cannot be put on hold for the possible infraction of civil rights. One legal scholar contends that "for law-abiding citizens, the benefits of a secure nation far outweigh the infrequent risks to one's individual expectation of private communications."[104] This scholar, however, fails to see the necessity of the constitutional safeguards which define the very structure of American government. The very system of this government is founded on the idea that "law abiding" individuals should not fear government intrusion, even if such intrusion is "infrequent." Any need for national security cannot overlook the letter of the law. In the case of electronic surveillance, an acceptable constitutional balance between civil liberties and national security was reached with the passage of FISA. Any extension of executive power that was invented

---

[102] *Ibid.*

[103] *Ibid.*

[104] Brown, "ECHELON."

by the notion of tacit Congressional approval clearly violations this important and fragile constitutional balance.

Works Cited

The 9/11 Commission Report. The National Commission on Terrorist Attacks Upon the United States. July 22, 2004. Public Law 107-306. http://www.9-11commission.gov /report/index.htm.

"ACLU Applauds House Introduction of FISA Oversight Bill." American Civil Liberties Union. *Safe and Free.* http://www.aclu.org/safefree/general/16872prs20030611.html. June 11, 2003.

Berge, Kari, ed. "Electronic Surveillance Warrant Procedures." *State Wiretapping Procedure Laws.* National Conference of State Legislatures. http://www.ncsl.org/ programs/lis/CIP/wiretap-proc.htm.

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

Brown, Erin L. "ECHELON: The National Security Agency's Compliance with Applicable Legal Guidelines in Light of the Need for Tighter National Security." *CommLaw Conspectus*. 2003. 1 CommLaw Conspectus 185.

"Church Committee Report." U.S. Congress. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights f Americans.* 94th Congress. 1st Session. April 23, 1976.

Copeland, Rebecca A. "War on Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America." *Texas Tech Law Review*. 35 Tex. Tech L. Rev. 1. (2004).

Cole, David and Martin S. Lederman. "The National Security Agency's Domestic Spying Program: Framing the Debate." *Indiana Law Journal*. Fall, 2005. 81 Ind. L.J. 1355.

Dash, Samuel. *The Intruders: Unreasonable Searches and Seizures from King John to John Ashcroft.* Rutgers University Press: New Brunswick, 2004.

Davis, Robert N. “Striking the Balance: National Security vs. Civil Liberties.” *Brooklyn Journal of International Law*. 2003. 29 Brooklyn J. Int'l L. 175.

Dempsey, Jim, Alan Davidson and Jerry Berman. “DOJ Proposes Further Surveillance Expansion Changes to Intelligence Authorization Would Again Increase FISA Eavesdropping.” Center for Democracy and Technology. CDT Preliminary Analysis. November 30, 2001. http://www.cdt.org/security/011130cdt.shtml.

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

Eggen, Dan. 2007. “Court Will Oversee Wiretapping Program: Change Does Not Settle Qualms about Privacy.” *The Washington Post,* January 18. A01.

Froomkin, Dan. 2007. “Bush: No Retreat on Spying.” *The Washington Post*. January 19. www.thewashingtonpost.com.

Goodwin, Jannan, Robert D. Boerner and Susan Frederick. “Electronic Surveillance.” *Protecting Democracy: States Respond to Terrorism.* National Conference of State Legislatures. http://www.ncsl.org/programs/press/2002/issues/surveillance.htm; and

Hoffman, Grayson A.. “Litigating Terrorism: The New FISA Regime, the Wall, and the Fourth Amendment.” *American Criminal Law Review*. Fall, 2003. 40 Am. Crim. L. Rev. 1655.

In re Sealed. 310 F.3d 717.

Katz v. United States. 389 U.S. 347, 358 (1967).

The Legal Authority for NSA Surveillance. December 22, 2005. Department of Justice Letter from Asst. Attorney General William E. Moschella to Congress.

Morton v. Mancari. 417 U.S. 535 (1974).

Murphy, Kathleen. “States Go Slow on Wiretap Expansion.” *Stateline.org*. Pew Research Center. October 12, 2001. http://www.stateline.org/live/ViewPage.action?siteNodeId=136&languageId=1&contentId=14507.

The National Security Agency’s Domestic Spying Program. January 9, 2006. Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department Letter of December 22, 2005.

Olmstead v. United States. 279 U.S. 849 (1929).

Seamon, Richard Henry and William Dylan Gardner. “The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement.” Harvard Journal of Law & Public Policy. 28 Harv. J.L. & Pub. Pol'y 319. (Spring, 2005).

Silverman v. United States. 365 U.S. 505 (1961).

Sims, John Cary. “What NSA Is Doing ... and Why It's Illegal.” *Hastings Constitutional Law Quarterly*. Winter / Spring, 2006. 33 Hastings Const. L.Q. 105.

Theoharis, Athan. “FBI Wiretapping: A Case Study of Bureaucratic Autonomy.” *Political Science Quarterly.* Vol. 107. No 1. (Spring 1992). Pg 104.

United States v. Duggan. 743 F.2d 59 (1984).

United States v. United States District Court for the Eastern District of Michigan, et al. 407 U.S. 297 (1972).

Wong, Katherine. “Recent Development: The NSA Terrorist Surveillance Program.” *Harvard Journal on Legislation*. Summer, 2006. 43 Harv. J. on Legis. 517.

Yoo, John C.. “Judicial Review and the War on Terrorism.” *The George Washington Law Review*. December, 2003. 72 Geo. Wash. L. Rev. 427.