Strategy Research Project

Tapping into the Wiretap Debate

by

Lieutenant Colonel David W. May
United States Army

United States Army War College
Class of 2012

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
03-02-2012	Strategy Research Project	

4. TITLE AND SUBTITLE
Tapping into the Wiretap Debate

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel David W. May

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Dr. Stephen Gerras
Department of Command, Leadership, &
Development

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution: A

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The use of electronic surveillance by federal intelligence agencies has historically been a contested topic. After a series of missteps by the intelligence community, Congress enacted the 1978 Foreign Intelligence Surveillance Act and Court to define and oversee electronic collection and surveillance in order to better protect civil liberties. In the twenty years that followed, the world would undergo an evolution in communication technologies, creating vulnerabilities for U.S. intelligence agencies under the law. In the aftermath of 9/11, both Congress and the Executive Office enhanced electronic surveillance measures to combat terrorism. Critics of the new laws and secret executive program argue infringements of civil liberties under the fourth Amendment. Advocates claim an essential need for national security. This paper will examine several related issues. What is the historical rationale behind the laws? How and why have they been adapted over time? Are they currently sufficient to provide intelligence agencies with the tools necessary to protect America while also providing adequate assurances to the American people of their right to privacy? And what further measures can be taken to improve the current system?

15. SUBJECT TERMS
Electronic Surveillance, Intelligence, Civil Liberties, Fourth Amendment, Security, FISA, USA PATRIOT ACT, President's Surveillance Program, FISC

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	32	

USAWC STRATEGY RESEARCH PROJECT

TAPPING INTO THE WIRETAP DEBATE

by

Lieutenant Colonel David W. May
United States Army

Dr. Stephen Gerras
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel David W. May

TITLE: Tapping into the Wiretap Debate

FORMAT: Strategy Research Project

DATE: 2 February 2012 WORD COUNT: 6,449 PAGES: 32

KEY TERMS: Electronic Surveillance, Intelligence, Civil Liberties, Fourth Amendment, Security, FISA, USA PATRIOT ACT, President's Surveillance Program, FISC

CLASSIFICATION: Unclassified

The use of electronic surveillance by federal intelligence agencies has historically been a contested topic. After a series of missteps by the intelligence community, Congress enacted the 1978 Foreign Intelligence Surveillance Act and Court to define and oversee electronic collection and surveillance in order to better protect civil liberties. In the twenty years that followed, the world would undergo an evolution in communication technologies, creating vulnerabilities for U.S. intelligence agencies under the law. In the aftermath of 9/11, both Congress and the Executive Office enhanced electronic surveillance measures to combat terrorism. Critics of the new laws and secret executive program argue infringements of civil liberties under the fourth Amendment. Advocates claimed an essential need for national security. This paper will examine several related issues. What is the historical rationale behind the laws? How and why have they been adapted over time? Are they currently sufficient to provide intelligence agencies with the tools necessary to protect America while also providing adequate assurances to the American people of their right to privacy? And what further measures can be taken to improve the current system?

TAPPING INTO THE WIRETAP DEBATE

> We reject as false the choice between our safety and our ideals. Our Founding Fathers, faced with perils we can scarcely imagine, drafted a charter to assure the rule of law and the rights of man, a charter expanded by the blood of generations. Those ideals still light the world, and we will not give them up for expedience's sake.
>
> —President Barak Obama[1]

Background

In the recent national deliberation over new laws to enhance America's security posture, the starting point of the discussion should be the recognition of two fundamental, yet often competing, national interests: the protection of our homeland and the safeguarding of our rights.[2] These core interests are identified in our founding documents – the U.S. Constitution and its Bill of Rights, as well as in our current National Security Strategy.[3] In the aftermath of the 9/11 attacks, as the nation began to seriously question the security of America's homeland for the first time since the Cuban Missile crisis, the country sought a strategic approach that at times placed these two enduring national interests at odds with each other.

While America is committed to being both free and secure, much of the debate has stemmed from what actions should be taken, whether or not those actions infringe on our civil liberties, and is there a need for some limited trade-offs. Unfortunately, the legality or constitutionality of these litigious matters is often argued from two extreme polarizing positions. I believe the opposing sides frequently distort the facts, often misrepresent the other side, and are unwilling to compromise. Such arguments make for big headlines, but are probably not the most effective means to advance the debate or build public policy.[4]

At the heart of the arguments are new laws and a secret Executive Office program designed to enable federal intelligence agencies and law enforcement officials, through electronic surveillance, to track down and punish those responsible for the 9/11 attacks while protecting America against any similar attacks in the future. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of October 2001, commonly referred to as the Patriot Act, The Protect America Act of 2007, and the Foreign Intelligence Surveillance Amendments Act (FAA) of 2008 are all recent regulations designed with this intent in mind. The President's Surveillance Program (PSP), a secret set of activities authorized by President George W. Bush in late 2001, also followed this aim without public knowledge.[5] While these laws and the PSP respond to a number of issues, one of the most contentious is granting federal officials greater powers to trace and intercept suspected terrorists' communications for both law enforcement and foreign intelligence purposes.[6] The dramatically reduced restrictions on electronic surveillance in particular, i.e. the ability to search telephone, e-mail communications, Short Messaging Service (SMS) traffic and other types of communications are among the key features that are troubling to some.

Some hard-line advocates of the 2001 legislation argue strongly that the laws and the PSP are desperately needed to meet the security challenges of the modern age. They reference leaders such as President George W. Bush who said "government has no higher obligation than to protect the lives and livelihood of its citizens,"[7] or noted abolitionist, Wendell Phillips, who stated, "Eternal vigilance is the price of liberty."[8] These advocates characterize liberal organizations such as the ACLU as undermining

the moral fabric of the country and inviting terrorism into America's borders.[9] As an example, three months after the attack on the World Trade Center and forty-one days after the Patriot Act went into law, Attorney General Ashcroft testified to the Senate Committee of the Judiciary by saying, "To those who scare peace-loving people with phantoms of lost liberty, my message is this: your tactics only aid terrorists, for they erode our national security and diminish our resolve. They give ammunition to America's enemies, and pause to America's friends. They encourage people of good will to remain silent in the face of evil."[10]

Critics of the laws and the PSP are no less severe in their commentary. They argue that the electronic surveillance provisions of the Patriot Act, certain aspects of follow-on regulations, and especially the President's Surveillance Program are in blatant violation of the Fourth Amendment to the U.S. Constitution. They view the legislation and secret program as an unnecessary invasion of our freedoms and see the changes in the law as a move toward the dystopian society portrayed in George Orwell's novel, *Nineteen Eighty Four*. Because the laws and the PSP mandate secrecy in regards to some of their uses, civil liberties groups claim Americans may never know whether their privacy has been violated by law-enforcement investigators or intelligence agencies relying on the Acts' powers.[11] Their position can be summed up by one of Benjamin Franklin's famous quotations, "They that who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety".[12]

This paper will examine several related issues involving the United States' use of electronic surveillance for foreign intelligence purposes. It will discuss the evolution of laws that govern this practice as well as the historical context and intelligence agency

missteps which served as the rationale for the creation and modification of such legislation. Further, the paper will analyze whether or not the current laws are sufficient to protect America without advocating the loss of civil liberties. Finally, it will offer recommendations for improving the system.

Definitions

In order to properly and critically analyze the merits and concerns of the enhanced electronic surveillance measures provided under the President's Surveillance Program and recent Congressional legislation, one must first understand the definitions of the key terms, the case law that provides the context, the historical abuses by the federal agencies which cause civil liberties groups to remain skeptical, and the changes in technology that affect the way intelligence agencies conduct business. With this framework in mind, an informed person can then judge whether or not the laws, which have been modified multiple times since 2001, provide a balance between our constitutional rights and the security of our nation.

The framework of the current regulations regarding electronic surveillance and its relationship to the fourth amendment can be found from a review of related case law. First and foremost, explanations of both the term 'electronic surveillance' and the essence of the Fourth Amendment are necessary. The Foreign Intelligence Surveillance Act (FISA) of 1978 provides a very specific definition of electronic surveillance which will be detailed later in this paper. Suffice for historical purposes, electronic surveillance, or wiretapping, can be described as any interception of a telephone transmission by accessing the telephone signal itself, and eavesdropping or listening in on conversations without the consent of the parties.[13] The Fourth Amendment, part of the Bill of Rights, guarantees "the right of the people to be secure in

their person's, houses, papers, and effects, against unreasonable searches and seizures… 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."[14]

Three other definitions are useful in this discussion: a United States person, a foreign power, and an agent of a foreign power. A U.S. person is any of the following: a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association with a substantial number of members that are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States. U.S. flagged ships and aircrafts are also protected as U.S. persons. A U.S. person does not include a corporation or an association that is a foreign power.[15] A foreign power can be one of several entities: a foreign government or any component thereof, a faction of a foreign government, an entity openly acknowledged to be directed and controlled by a foreign government, or a foreign-based political organization. An agent of a foreign power is an officer or employee of a foreign power, or a spy, terrorist, saboteur, aider, abettor, or conspirator.[16]

Historical Context and Abuses of Authority

The first of two major decisions made by the Supreme Court regarding the nature of the "right to privacy" and the legal definition of "search" as it applies to electronic surveillance occurred in 1928, during the case of Olmstead vs. the United States. This was the era of prohibition, and Mr. Olmstead was accused of illegally transporting and distributing alcoholic beverages from Canada to the United States. During the investigation, law enforcement officers, who suspected Mr. Olmstead of bootlegging,

wire-tapped his home phone, his office phone, and a building which he owned. They collected his communications, arrested him, and then used his seized communications as evidence during the trial. Mr. Olmstead argued that his Fourth Amendment rights had been violated.[17] In a landmark decision, the Court ruled that that the obtaining of evidence and its use at the trial did not violate the fourth amendment. Because the communications traveled by wire, outside of Mr. Olmstead's premises, the Court determined that there is no expectation of privacy.[18] Hence the Supreme Court ruled that electronic communications were not protected by the fourth Amendment, and so ushered in the 'Golden Age' of electronic surveillance where the government could collect communications at will.

The second case, Katz vs. the United States, occurred almost four decades later, in 1967. The accused stood trial for making illegal gambling bets. Mr. Katz would make use of a public phone booth to conduct his illicit business, so the police placed a surveillance device on the top of the booth whereby they collected his communications. Similar to the Olmstead case, police seized the communications, arrested Mr. Katz, and brought him to trial. Mr. Katz also argued that his fourth amendment rights had been violated. This time, the Supreme Court overturned its previous decision.[19] Justice Stewart ruled, "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[20] Additionally, the justice ruled that regardless of location, a conversation is protected from unreasonable search and seizure under the Fourth

Amendment if it is made with a reasonable expectation of privacy. Further, wiretapping was considered a search.[21]

The following year Congress passed The Omnibus Crime Control and Safe Streets Act of 1968, also known as the Wiretap Act, requiring the government to obtain a search warrant in order to collect and search electronic communications. However, the Katz case and the Wiretap Act dealt with communications primarily within a law enforcement context. In fact, the Wiretap Act specifically excluded National Security surveillance from its coverage. Section 2511(3) specified that nothing in the Wiretap Act shall limit the constitutional power of the President "to take such measures as he deems necessary to protect the nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States or to protect national security information against foreign intelligence activities."[22] So the 'Golden Age' of electronic surveillance continued a little longer.

During this 'Golden Age', the Army and the National Security Agency operated in a sort of legally permissive environment. They conducted several operations that could be argued were not in the best interest of its citizens. Three programs in particular provided the basis for much of the public distrust of the government's use of electronic surveillance and led to the creation of the Foreign Intelligence Surveillance Act of 1978.

The first program was known as Project Shamrock (1945 – 1975). During World War II the U.S. Army had the authority to read and censor all telegram traffic going into and out of the United States for the purpose of identifying persons divulging military secrets and committing espionage. This practice continued after the war by the Armed

Forces Security Agency (AFSA) and was turned over to the National Security Agency (NSA) upon their establishment in 1952. Under the program, virtually all international telegrams sent and received by major telecom carriers were provided to NSA. In the later years, approximately 150,000 telegrams a month were reviewed by NSA analysts. If the information was of interest to other intelligence agencies, NSA would share the material. Messages were disseminated to the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), the Bureau of Narcotics and Dangerous Drugs (BNDD), the Secret Service, and the Department of Defense (DOD). There was no court oversight nor were warrants required. Congress eventually learned of and exposed the program, which was then terminated in 1975. The major problem with this method is it constituted a vacuum approach or general search. There was no specific signals intelligence mission guiding the effort, rather the AFSA and NSA were indiscriminately reading through large amounts of traffic derived from U.S. persons. During a congressional hearing, the Senate Intelligence Committee concluded the program was, "probably the largest government interception program affecting Americans ever undertaken."[23]

The second program was code named Project Minaret, a.k.a. The Watch List (1967-1973). This effort took place during great turmoil within the United States. The U.S. government was concerned over anti-Vietnam war protests, civil rights marches, the burning of ROTC buildings on college campuses, and other civil unrest. So the Executive Branch, law enforcement and intelligence agencies (CIA, DIA, and FBI) compiled watch lists and passed them to NSA to target international communications associated with foreigners, organizations, and American citizens who were active in the

anti-war and civil rights movements. Names of U.S. persons were used systematically as a basis for selecting messages. Among the notables on the watch list were Jane Fonda, Martin Luther King Jr., Joan Baez, and Dr. Benjamin Spock. Over 3,900 reports were issued on watch-listed U.S. persons according to the NSA Director, Lew Allen's testimony before the Senate Intelligence Committee in 1975. Although the Supreme Court confirmed the U.S. government's authority to protect the nation from subversive activity and anarchy, political speech was protected under the constitution. The controversy of Project Minaret questioned the government's ability to use electronic surveillance for domestic espionage purposes without judicial oversight or warrants for interception.[24]

The third program involving electronic surveillance took place from 1970 to 1973 at the request of the Bureau of Narcotics and Dangerous Drugs (BNDD), the predecessor agency to the Drug Enforcement Agency (DEA). The BNDD was attempting to disrupt illicit narcotic shipments from South America into the United States. The drug deals were being arranged in telephone calls from public telephone booths in New York City to a South American City. Given the ruling on the Katz case and the Wire Tap Act of 1968 discussed earlier, The BNDD recognized that it could not legally tap the public telephones without a warrant. Since BNDD didn't know who exactly they were attempting to investigate, or what kind of evidence they were expecting to find, they did not want to risk having a judge deny the warrant request. Rather, they solicited NSA's assistance to monitor international communications linked to drug trafficking. In addition, BNDD submitted the names of 450 Americans to NSA for a "drug" watch list. This list resulted in the dissemination of about 1,900 reports on

drug traffickers to both BNDD and CIA. In essence, NSA was enabling BNDD law enforcement activities by identifying the drug traffickers in New York, thus facilitating their eventual arrest. What was wrong with this modus operandi? NSA has no law enforcement authority, and this program was serving a law enforcement function. NSA was helping BNDD evade a legal requirement for a search warrant. In June 1973, NSA came to view the program in its proper context, beyond the scope of its proper mission, and terminated the mission.[25]

Resulting Regulation and Oversight

These activities, in conjunction with alleged abuses of law by the CIA and FBI, caught the eye of certain members of Congress. In 1975, Congress established the 'United States Select Committee to Study Governmental Operations with Respect to Intelligence Activities' to investigate intelligence gathering for illegal purposes. The Church Committee, as it was commonly referred due to being chaired by Senator Frank Church, focused primarily on the CIA and FBI, but also brought the secretive world of the NSA and its electronic surveillance programs into the public eye. After extensive review of Projects Shamrock and Minaret, Church commented that the effort, "certainly appears to violate ... the fourth Amendment to the Constitution".[26] The Committee also noted that "at no time…were the Justice Department's standards and procedures ever applied to NSA's electronic monitoring system and its 'watch listing' of American citizens".[27]

A myriad of actions resulted or were inspired from the Church Committee hearings and other investigations that directly affected how intelligence agencies would conduct electronic surveillance in the future. First and foremost, the CIA, FBI, and NSA terminated all electronic surveillance activities that were considered illegal or out of

scope with their missions. Congress then passed the Foreign Intelligence Surveillance Act in 1978[28] and established the Foreign Intelligence Surveillance Court,[29] both of which provided the basis for intelligence oversight. In 1981, President Reagan signed executive order 12333, entitled United States Intelligence Activities. This order defined who was considered part of the intelligence community and specified the responsibilities for each member.[30] A year later, the Department of Defense (DoD) published its own regulation, 5240.1-R, which set forth procedures governing the activities of DoD intelligence components that affect United States persons.[31]

Both the FISA and EO 12333 codified the applicable legal standards for the collection, retention, and dissemination of information concerning U.S. persons using electronic surveillance for foreign intelligence purposes. They provided the guiding principles or foundational law by which all electronic surveillance is judged, even today. At the time, these documents reflected a careful balancing between the needs of the government for such intelligence and the protection of the rights of U.S. persons by closely regulating the conduct of electronic surveillance that either targets U.S. persons or might result in the acquisition of information to, from or about them.[32]

The FISA defines electronic surveillance as any one of four activities:

1) The acquisition of either wire or radio communications of a U.S. person located in the United States by targeting that individual;

2) The acquisition of wired communications to or from a person in the United States, without their consent, if the acquisition occurs in the United States;

3) The intentional acquisition of radio communications if all parties are physically located in the United States; or

4) Monitoring in the United States to acquire information other than from wire or radio.

To recap, electronic surveillance as defined by FISA pertains to acquisition of U.S. persons' communications or communications that routed into or out of the United States. Collecting communications of foreign powers or agents of a foreign power outside of the United States where the communications do not originate, terminate or are not routed through the United States is not considered electronic surveillance as defined by the FISA. This distinction is important, because the FISA requires government agencies to obtain either the approval of the Attorney General or an order from the Foreign Intelligence Surveillance Court before conducting electronic surveillance.[33]

In most circumstances, the FISA allows for electronic surveillance under two scenarios. The President, through the Attorney General, may approve electronic surveillance for a period of up to one year for the purposes of collecting foreign intelligence targeting foreign powers or their agents if there is low likelihood that the collection will contain U.S. persons' communications, i.e. non U.S. persons' communications collected in the United States. Alternatively, the government may seek a court order permitting the surveillance using the Foreign Intelligence Surveillance Court (FISC).[34]

The FISC was established by Congress under the FISA as one of several intelligence oversight measures. The Court originally consisted of seven federal judges who rotate through Washington D.C. to hear pleadings from government agencies seeking surveillance warrants related to national security investigations. The Court provides guidance as to the criteria and requirements which must be presented in the

warrant application process. Each application must contain evidence and the Attorney General's certification that the target of the surveillance is a foreign power or an agent of a foreign power, and in the case of a U.S. person that the target may be involved in the commission of a crime or acting as an agent of a foreign power.[35]

The FISC operates in almost total secrecy, its deliberations and decisions are closed to the public. A FISC judge can approve, deny or request modification of an application. If an application is rejected by one FISC judge, the government is not allowed to resubmit the application to a different FISC judge. Rather these denials must be appealed to the United States Foreign Intelligence Court of Review. Such appeals are extremely rare, with the first appeal submitted 24 years after the creation of the FISC. Outright denials of applications are also extremely uncommon; rather, the court has historically requested a modification to the original request when there was a point of concern. In emergency situations, the Attorney General may authorize electronic surveillance; however, the FISC must be notified within 72 hours after such authorization.[36] In 1980, the first full year after its inception, FISC approved 322 warrants and denied zero. The number of applications has steadily risen over the years, reaching over 2000 for a single year in 2005. In the last 30 years (1980 through 2010) the court has approved 30,135 applications (sometimes with modifications; or with the splitting up, or combining together, of warrants for legal purposes) and rejected only 11.[37]

With a 99.96% approval rating and all proceedings closed to the public, it's not difficult to surmise why many critics question the validity of the court's oversight role. But as a seasoned cryptologist with 13 years serving with the National Security Agency,

I can attest that the system provides more than adequate oversight. The reason for the exceedingly high approval rate is not due to the leniency of the court, but rather the emphasis analysts place on submitting only those applications that provide more than sufficient evidence and justification to ensure the court's endorsement. Because the intelligence agencies have a less-than-stellar historical reputation for supporting civil liberties, they now tend to overcompensate when submitting applications. The intelligence system frowns upon any analyst who puts forward a sub-standard request to the court, as the analyst's reputation and opportunities for career advancement are at stake. Multiple reviews take place before the application is forwarded. The resulting process is less timely than originally designed by Congress, because of the deliberate bureaucracy created by the intelligence agencies' internal procedures.

Without question, the Church Committee hearings produced positive results through regulations and oversight created to safeguard the civil liberties of its citizens. However, the hearings had another unintended and arguably unconstructive outcome. By openly divulging and criticizing all of the questionably inappropriate activities conducted by the federal law enforcement and intelligence agencies during the 'Golden Age' of electronic surveillance, Americans lost faith in the organizations that were designed to protect them. Public trust was lost, reputations were damaged. This distrust would create the conditions that would eventually hinder the U.S. intelligence agencies' ability to protect America from a future attack.

A National Crisis and Modifications to the Law

For over twenty years FISA regulations and congressional oversight measures of electronic surveillance for foreign intelligence purposes stood unaltered despite an evolution in telecommunication technologies. American businesses dominated the

environment, and the U.S. became the global leader in information and communication technologies services sectors as well as in telecommunications technology infrastructure.[38] Much of the world's international telephone and e-mail traffic was being routed through hubs residing on U.S. soil and owned by U.S. firms. This posed a huge challenge for American intelligence agencies, especially NSA, because communications collected in the U.S., even international communications where both parties resided outside the U.S., required a warrant under FISA. Adversaries began to manipulate their communications in such a way that would provide them protection under the 1978 law, thus giving them a decisive advantage in eluding intelligence collection. Federal intelligence agencies were unable to convince Congress or the American people, who were highly suspicious of their activities due to past discretions, that the current laws did not foresee nor take into account the technology progression which was creating advantages for our adversaries. Congress felt the legislation was sufficient to ensure the protection of civil liberties while allowing the intelligence agencies adequate flexibility to accomplish their mission. NSA, CIA, and the FBI grappled with ways to improve their capabilities under the current legal framework against enemies who were exploiting every opportunity in the continually changing telecommunications environment.

The terrorist attacks of September 11, 2001 caused many in the federal government to finally recognize the intelligence community was handcuffed by legal and bureaucratic restrictions and not effectively poised to take advantage of the current technological environment. The Patriot Act was Congress' attempt to address many of these shortcomings. The Act eased many of the restrictions on foreign intelligence

gathering within the United States and provided the U.S. intelligence community greater access to information discovered during criminal investigations. The sections of FISA authorizing electronic surveillance without a court order specifically excluded their application to groups engaged in international terrorism.[39] The Patriot Act amended those sections to include terrorism on behalf of groups that are not specifically backed by a foreign government. In terms of electronic surveillance in particular, the scope and availability of wiretapping and surveillance orders were increased, but the law also established and expanded additional safeguards against official abuse.[40]

Among its many provisions, the Patriot Act increased the number of judges on the FISA Court from seven to eleven, to speed review and oversight of FISA surveillance applications. Under the new law, FISC applications now allowed for a search order when gathering foreign intelligence was "a significant reason" rather than the sole rationale for the request. The Patriot Act also authorized pen register and trap & trace device orders for email as well as telephone conversations. Pen register and trap & trace are electronic devices used to record and trace numbers, email, and communication signals from a telecommunication system. Wiretaps were expanded to include addressing and routing information to allow surveillance of packet switched networks, a common communications technology that did not exist when FISA went into law. The law also permitted "roving wiretaps", or court orders that do not need to specify all locations, devices, or service providers.[41] Roving wiretaps, highly controversial at the time, were deemed essential to tracking terrorists. Operational security (OPSEC) savvy terrorists were actively exploiting the law by rapidly changing locations and communications devices, which previously required a modification to the

court order.[42] Although critics saw roving wiretaps as violating the particularity clause of the Fourth Amendment, congress extended this provision of the law on several occasions, most recently on May 26, 2011.[43]

The safeguards of the Patriot Act included a number of sunset provisions requiring certain sections of the law to be revisited and extended through new legislation or they would cease to have effect. Most temporary provisions were originally set to expire on December 31, 2005, with the roving wiretap being one such example. The law also established a claim process against the federal government for certain privacy violations by government personnel. Further, the law now required that no investigation could be undertaken on citizens who were carrying out activities protected by the First Amendment,[44] a lesson learned from Project Minaret.

Executive Authority

President George W. Bush signed the Patriot Act into law, but apparently did not believe the legislation went far enough to protect America, because he elected to secretly undertake additional security measures against terrorism. In the weeks following 9/11, the President authorized NSA to conduct a number of new, highly classified intelligence activities that only recently became known to the public. Most details of the specific intelligence activities remain highly classified. However in December 2005, following a series of articles published in the New York Times, the President and other Administrative officials publicly acknowledged that the activities included allowing NSA to conduct electronic surveillance within the United States on U.S. persons without a FISC court order when certain factual conditions and legal standards were met.[45] The specific publicly disclosed NSA activity was referred to by

the President as the “Terrorist Surveillance Program” (TSP) while the compilation of all the classified activities became known as the President’s Surveillance Program (PSP).[46]

Few knew of the PSP’s existence, and access for non-operational personnel was tightly restricted at the direction of the White House. The program was reauthorized every 45 days by the President and changed over time. During each reauthorization hand-selected members of the DOJ would review the program and include a finding specifying that an extraordinary emergency continued to exist and that the circumstances “constitute[d] an urgent and compelling governmental interest” to justify the activities without a court order.[47] The overly restrictive access of the program prevented the DOJ from adequately reviewing the PSP’s legality during the earliest phases of its operations. The sole legal opinion used to support the inception of the program was drafted by DOJ Office of Legal Counsel (OLC) Deputy Assistant Attorney General John Yoo, the “White House’s guy on Security matters.”[48] Successors in the OLC who were read-in years later identified a number of deficiencies in the opinion that eventually led them to reassess the program’s legality.[49] In early 2004, DOJ concluded that certain aspects of the program were not supported by law and advised the President that the program should be modified. On March 11, 2004 the White House attempted to push forward new Presidential Authorizations certified by the White House Counsel without DOJ concurrence, claiming the President’s use of his Article II Commander-In-Chief authority superseded any contrary provisions of the law, including FISA. After several senior DOJ and intelligence officials threatened to resign, the White House eventually acquiesced and made modifications to the program.[50]

The impact of the PSP on intelligence community counterterrorism efforts may never be fully known to the public. From 2004 to 2006 certain activities originally authorized under the PSP were transitioned to the FISC. As a result, the final PSP authorization expired in early 2007. The White house stated that the transition of authority over the two year period addressed the Administration's concerns about preserving the speed and agility of program. NSA Director, General Hayden, stated that portions of the PSP were important to NSA efforts to defend the nation. Many senior intelligence officials felt that the PSP covered a seam between foreign and domestic intelligence domains.[51] Critics of the program believed it was unnecessary, because a warrant based system through the FISC already existed which allowed federal intelligence agencies to eavesdrop on U.S. persons inside the United States who might be tied with terrorist groups without circumventing longstanding rules.[52] They also argued that activities affecting U.S. persons' civil liberties should not be kept secret and should require appropriate checks and balances from the other branches of government.

Without question, the collection activities pursued under the PSP were unprecedented and drew into question the seemingly over-extensive authority of the Executive Branch without counterbalances as designed by the forefathers. While conflicting views surrounding the legality of the PSP exist, an estimated forty lawsuits were filed alleging that the Bush administration illegally monitored their phone calls or e-mails.[53] A DOJ Inspector General investigation stated that it was inappropriate for a single attorney to be relied upon to conduct the initial legal assessment of the PSP, and the lack of oversight and review contributed to a legal opinion that "at a minimum" was

factually flawed. Further, the investigation concluded that the White House's strict controls over access undermined DOJ's ability to perform its critical legal functions.[54]

In August of 2007 the Protect America Act (PAA) was passed and amended FISA to address the government's ability to conduct electronic surveillance within the United States on persons reasonably believed to be located outside of the country.[55] PAA expired in early 2008, however it was reenacted in a slightly modified form several months later through the FISA Amendments Act of 2008. This latter law gave federal agencies the authority to intercept any communications inside the United States associated with non-U.S. persons reasonably believe to be located outside the United States, when a significant purpose of the acquisition pertains to foreign intelligence. The Act gave the government broader authority than the provisions allowed by the secretive President's Surveillance Program when intercepting international communications; however, it also provided safeguards for U.S. persons. Under the Amendment, all government agencies are required to obtain a court order to conduct surveillance on U.S. persons residing overseas.[56]

After seven years, a covert executive program, several large pieces of controversial legislation, numerous lawsuits, and a heated public debate, Congress finally enacted a law that provides the U.S. intelligence community with the necessary authorities to respond to terrorist and other foreign threats while safeguarding civil liberties. The FISA Amendment Act of 2008 draws from all of the previous electronic surveillance lessons learned, and assigns critical roles to each branch of government to balance power. The Attorney General and the Director of National Intelligence are charged with ensuring law enforcement and intelligence agencies work together in

collecting foreign intelligence according to the law. The Amendment Act requires the FISA Court to review and approve orders based on probable cause for targeting Americans regardless of their location on the globe to ensure actions are consistent with the Fourth Amendment, while allowing collection of foreign intelligence without a court order regardless of point of collection. And the Amendment calls for regular reporting to Congress to ensure the Legislative Branch fulfills its oversight responsibilities.[57]

Recommendations

Despite tremendous accomplishments over the last decade, Federal intelligence agencies continue to have a tainted reputation, in large part due to their historical missteps and alleged past abuses of authority. General public distrust is not easily overcome, and this doubt breeds suspicion whenever new rules are requested to keep pace with technological advancements or adversaries' changing tactics. While America's security necessitates that intelligence agencies conceal their sources and methods, more should be done to tout intelligence successes and build their reputation in the public eye. A logical step would be to change the intelligence community's culture from media avoidance to embracement. Opportunities for recognition are often missed, because intelligence professionals are constantly indoctrinated not to disclose any information or speak to the media. At a minimum, Senior Intelligence officials and their associated public affairs offices should engage in an information campaign that acknowledges achievement while managing risk. With an improved reputation, the public wouldn't be so quick to question or scrutinize changes to regulations.

With regard to the law, all regulations that govern intelligence activities with respect to U.S. persons should be a matter of public record. Further, Congress must be cognizant of how much power they grant the Executive Branch during extreme

circumstances. The President's Surveillance Program brought into question the authority of the Executive Branch to act without oversight. In this circumstance, the checks and balances designed within the Constitution were skirted. The Bush Administration believed that the Authorization for the Use of Military Force (AUMF) passed by the Congress shortly after 9/11 gave the President authority to use both "all necessary and appropriate force" both domestically and abroad including signal intelligence capabilities to prevent terrorist attacks against the United States. The Administration understood the AUMF to provide an express authorization to conduct targeted electronic surveillance against al-Qa'ida and its associates and thus supported the President's directives to conduct clandestine activities under the PSP.[58] However, the FISC court procedures offered similar capabilities under the law, and a FISC court order could be granted within hours of a request under emergency circumstances. In reality, the Bush Administration favored speed, efficiency, and reduced oversight to the existing bureaucratic process that ensured the protection of civil liberties. It's interesting to note that the IG report questioning the PSP's legality was only released publically after President Bush left office, even though the program was discontinued several years earlier.

Another method to advance accountability of intelligence collection would be to replace certain aspects of the current oversight process with compliance programs and training. There is precedence for this practice as Congress employs compliance programs for education (No child Left Behind), the healthcare industry (Healthcare Reform Law) and the banking industry. The intelligence community already uses mandatory training programs extensively, although most requirements are derived from

internal policies and rather than Congressional law. Nesting internal procedures with Congressional regulations would reduce bureaucracy. Rather than have the FISC review and approve each and every FISA application, the court could selectively spot check to ensure compliance within existing laws. Such a practice would dissolve the requirement to seek out a judge for every FISA related electronic surveillance activity, speed the process of intelligence collection, and place the onus on the intelligence agencies to ensure their personnel are properly trained to compliance standards.

The law makers who wrote the Foreign Intelligence and Surveillance Act of 1978 did not take into account the fact that in twenty years most of the world's communications would be digital, packet based, and frequently routed through the same network infrastructures as U.S. Persons' communications. General suspicion of historical intelligence activities hampered necessary changes to the law. Hence, the intelligence community was ill prepared to respond when the Nation was attacked on September 11, 2001. Three actions are required to ensure this doesn't happen again. First, laws need to be written is such a manner as to recognize that technology will change and the methods used to exploit the technology must change as well. Sunset clauses should be included as an appropriate measure to guarantee intelligence legislation is revisited and modified as necessary. Fortunately, the FISA Amendment Act of 2008 has a sunset clause which is set to expire at the end of 2012.[59] Secondly, select members of the Congress and Judicial Branches must be familiar enough with current and emerging technology to ensure the appropriate language is addressed in future legislation. Lastly, the American people must recognize that despite the missteps of the past, the intelligence community is working tirelessly to protect them from harm

as well as protect their freedom and civil liberties. Intelligence leaders at all levels, from the Director of National Intelligence to the section supervisor, endeavor to work within the parameters of the law. The debate should be about the laws that provide the security for our nation, not the professionals that carry it out.

Endnotes

[1] Barak Obama, *Inaugural Address*, Washington, D.C., Capital Building, 20 January 2009, http://www.whitehouse.gov/blog/inaugural-address (accessed December 23, 2011).

[2] Amitai Etzioni, *How Patriotic is the Patriot Act,* New York, NY, Routledge, 2004) 1.

[3] The National Security Strategy of the United States of America, May 2010, 7.

[4] Etzioni, 1-2.

[5] James Risen and Eric Lichblau, "Bush Let's U.S. Spy on Callers Without Courts," New York Times, December 16, 2005.

[6] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (H.R. 3162), http://thomas.loc.gov/cgi-bin/bdquery/z?d107:H.R.3162.

[7] George W. Bush, The National Security Strategy of the United States of America, March 2006, 12.

[8] Wendell Phillips, Speech in Boston, Massachusetts, January 28, 1852, *Speeches before the Massachusetts Anti-Slavery Society*, 1853, 13.

[9] Etzioni, 2.

[10] John Ashcroft, Testimony to the Senate Committee on the Judiciary, December 6, 2001.

[11] Larry Abramson, "The Patriot Act: Alleged Abuses of the Law," NPR, http://www.npr.org/templates/story/story.php?storyId=4756403, (accessed November 19, 2011).

[12] Benjamin Franklin, *An historical Review of the Constitution of Government of Pennsylvania* (London, R. Griffiths, 1759) 289.

[13] National Conference of State Legislatures, Electronic Surveillance Laws, 29 August 2010, http://www.ncsl.org/default.aspx?tabid=13492, (accessed November 16, 2011).

[14] U.S. Constitution, Amendment 4.

[15] United States Code, Title 50, 1801(i).

[16] Foreign Intelligence Surveillance Act, 1978, http://uscode.house.gov/download/pls/50C36.txt, (accessed November 14, 2011).

[17] Olmstead v. United States, 277 U.S. 438 (1928). http://www.law.cornell.edu/supct/html/historics/USSC_CR_0277_0438_ZS.html.

[18] Olmstead v. United States, 277 U.S. 438 (1928).

[19] Katz v. United States, 389 U.S. 237 (1967).

[20] Welsh S. White and James J. Tomkovicz. *Criminal Procedure: Constitutional Constraints upon Investigation and Proof* (Newark, NJ: LexisNexis Matthew Bender, 2004), 6.

[21] Katz v. United States.

[22] Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351, 1968, http://transition.fcc.gov/Bureaus/OSEC/library/legislative_histories/1615.pdf, (accessed October 17, 2011).

[23] John Ponder, Operation Shamrock: NSA's First Domestic Spy Program Was Revealed by Congress in 1975, *Pensito Review*, May 13, 2006., http://www.pensitoreview.com/2006/05/13/operation-shamrock-nsas-first-domestic-spying-program-was-shut-down-by-congress-in-1975/, (accessed on November 11, 2011).

[24] Katelyn Epsley-Jones and Christina Frenzel, The Church Committee Hearings and the FISA Court, *Frontline*, PBS, May 15 2007, http://www.pbs.org/wgbh/pages/frontline/homefront/preemption/churchfisa.html, (accessed November 13, 2011).

[25] 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*, Book III, 23 April 1976, available from http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportIIIj.htm, (accessed November 29, 2011).

[26] Epsley-Jones and Frenzel, The Church Committee Hearings and the FISA Court.

[27] U.S. Congress, *Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans.*

[28] Foreign Intelligence Surveillance Act, 1978.

[29] Federal Judicial Center, Foreign Intelligence Surveillance Court, http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html (accessed November 14, 2011).

[30] Executive Order 12333, United States Intelligence Activities, Federal Register, National Archives, http://www.archives.gov/federal-register/codification/executive-order/12333.html, (accessed November 14, 2011).

[31] DoD Regulation 5240.1-R, Procedures governing the activities of DoD intelligence components that affect United States persons, 1982.

[32] National Security Agency, “Legal Standards for the Intelligence Community in Conducting Electronic Surveillance”, February 2000, http://www.fas.org/irp/nsa/standards.html, (accessed December 1, 2011).

[33] Foreign Intelligence Surveillance Act, 1978.

[34] Ibid.

[35] Federal Judicial Center, “Foreign Intelligence Surveillance Court,” http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html, (accessed December 12, 2011).

[36] Foreign Intelligence Surveillance Act, 1978.

[37] Electronic Privacy Information Center, “Foreign Intelligence Surveillance Act Court Orders 1979-2010,” http://epic.org/privacy/wiretap/stats/fisa_stats.html, (accessed December 14, 2011).

[38] Office of the United States Trade Representative, “Telecom and E-Commerse”, http://www.ustr.gov/trade-topics/services-investment/telecom-e-commerce, (accessed December 23, 2011).

[39] USA PATRIOT ACT, 2001.

[40] Charles Doyle, CRS Report for Congress, “The USA PATRIOT ACT: A Sketch”, Congressional Research Service, The Library of Congress, April 18, 2002, 1-3.

[41] Foreign Intelligence Surveillance Act, 1978. Title II.

[42] Doyle, 3.

[43] Michael Winter, “Senate votes to extend Patriot Act's roving wiretaps, records search”, USA Today, May 26, 2011, http://content.usatoday.com/communities/ondeadline/post/2011/05/senate-votes-to-extend-patriot-act-anti-terror-provisions/1, (accessed December 23, 2011).

[44] Doyle, 3.

[45] Risen and Eric Lichblau, “Bush Let’s U.S. Spy on Callers Without Courts”.

[46] Department of Defense Office of the Inspector General et al., Unclassified Report on the President’s Surveillance Program (Washington, DC: Office of the Inspector General, January 2010) 1 - 5.

[47] Ibid, 6.

[48] Ibid, 5-11.

[49] Pamela Hess, “Presidential Surveillance Program,” The Huffington Post, November 11, 2009, http://www.huffingtonpost.com/2009/07/10/presidential-surveillance_n_229595.html, (accessed December 27, 2011).

[50] Dan Eggen and Paul Kane, “Gonzales Hospital Episode Detailed,” New York Times, May 16, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR2007051500864.html, (accessed December 27, 2011).

[51] Department of Defense Office of the Inspector General et al., Unclassified Report on the President’s Surveillance Program, 30-32.

[52] Risen and Eric Lichblau, “Bush Let’s U.S. Spy on Callers Without Courts”.

[53] Eric Lichblau, “Deal Reached in Congress to Rewrite Rules on Wiretapping,” New York Times, June 20, 2008, http://www.nytimes.com/2008/06/20/washington/20fisacnd.html, (accessed Dec 28, 2011).

[54] Department of Defense Office of the Inspector General et al., “Unclassified Report on the President’s Surveillance Program,” 30.

[55] Protect America Act of 2007, Public Law 110-5, 110th Congress, http://intelligence.senate.gov/laws/pl11055.pdf, (accessed December28, 2011).

[56] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, H.R. 6304 [110th Congress, http://www.govtrack.us/congress/billtext.xpd?bill=h110-6304, (accessed December 28, 2011).

[57] Kit Bond, “FISA Amendments Act of 2008”, The Wall Street Journal Online, June 19, 2008, http://online.wsj.com/article/SB121391360949290049.html, (accessed December 28, 2011).

[58] Department of Defense Office of the Inspector General et al., Unclassified Report on the President’s Surveillance Program, 29-30.

[59] Bond, “FISA Amendments Act of 2008”.