The PATRIOT Act: Amending the Foreign Intelligence Surveillance Act and Diminishing Civil Liberties

Krisda Chaiyachati
Edmund Morrell
Sachin Varghese
To Dr. Johnson, the best special assistant to the chair of the Senate Select Committee on Intelligence and world leader on all things Intelligence, SPIA, and Kiwi
Table of Contents

Introduction ............................................................................................................. 1
Ambiguous Authority ......................................................................................... 1
COINTELPRO .................................................................................................... 8
Church Committee: Revelations of Abuse ......................................................... 12
Road to FISA ..................................................................................................... 14
The Foreign Intelligence Surveillance Act ......................................................... 17
The PATRIOT Act ............................................................................................ 26
The Turning Tide .............................................................................................. 35
Conclusion ......................................................................................................... 37
Appendices and Works Cited .............................................................................. 38


**Introduction**

The terrorist attacks of September 11, 2001 left an indelible mark and an overshadowing feeling of vulnerability. They also created a determination to respond to the new national security threats they represented. In its response, the United States must consider not only cumbersome national security interests, but also various rights and restrictions laid down by the Constitution and acts of Congress protecting Americans. The Federal Intelligence Surveillance Act (FISA) of 1978 sought to address these concerns by legitimizing the surveillance and investigation of individuals in the U.S. for the purposes of foreign intelligence. FISA establishes a system of secret courts that approve such investigations while maintaining the expediency required by the intelligence community. In the wake of the terrorist attacks of 2001, the Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (PATRIOT Act), the balance achieved by the FISA courts was—briefly—re-examined, and the interests of intelligence and national security were bolstered at the potential expense of domestic freedoms without significant increases in the accountability or oversight of domestic intelligence gathering. This suggests obvious questions: what is the legitimate function of U.S. intelligence within the domain of domestic affairs, and how should that process be overseen and made accountable to the U.S. people?

This paper will first investigate the constitutional and statutory history regarding the development of FISA, primarily focusing on Supreme Court decisions and the abuses of the FBI prior to FISA in order to provide, respectively, a legal context and a cogent foil to our present situation. Then it will turn to an examination of the history of FISA itself in order to provide a comprehensive account of its function. Finally, the PATRIOT Act will be studied, primarily in its relation to FISA and how it provided the Executive branch with unchecked powers.

**Ambiguous Authority: Warrants and National Security prior to FISA**

The Fourth Amendment provides,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probably cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. (U.S. Constitution)

This directive by no means provides immunity from all unwanted searches and seizures, but only those of a certain nature. The Amendment’s general meaning explicated by the Supreme Court is that evidence and information
collected by the government must be obtained in a reasonable manner and that the proper warrants are issued only after probably cause has been established. Ultimately, this interpretation requires warrants in most searches and seizures, even though it admits a number of exceptions (most strictly defined, some broadly—e.g. ‘objectively reasonable’) to the warrant clause.

Although originally drafted with criminal law enforcement investigations in mind, the Fourth Amendment is pertinent to the legitimate exercise of domestic intelligence gathering, as many, if not most, of the techniques used for criminal investigations are also used for intelligence gathering purposes. With two cases decided in 1967, the Supreme Court addressed these issues directed. First, in *Berger v. New York*, the Court determined that both wiretapping and eavesdropping were to be regarded as searches and that the intercepted communications were similarly considered seized materials—all falling under the general umbrella of the Fourth Amendment. Speaking for the Court, Justice Clark declared:

> By its very nature eavesdropping involves an intrusion on privacy that is broad in scope…[furthermore the] procedure, necessarily because its success depends on secrecy, has no requirements for notice as do conventional warrants, nor does it overcome this defect by some showing of special facts. (*Berger v. N.Y.*, 388 U.S. 41)

Even though the Court thus brought such methods of surveillance “fully within the purview of the Fourth Amendment,” requiring that as such they be generally more in line with the spirit of the Amendment, it was not until *Katz v. United States* was decided during the next session that physical trespass onto a “constitutionally protected area” was necessary to elicit Fourth Amendment warrant protection (*Berger v. N.Y.*, 388 U.S. 41; Ducat, 742). *Katz* signaled a full reversal of the Court’s prior reliance on physical intrusion and tangible seizures in regard to implementing the directives of the Amendment. Rather, it determined that “the Fourth Amendment protects people, not places;” that is, instead of extending protection against physical trespass, it extended it against the trespass of individual privacy (Elliff, 59-60). Moreover, the *Katz* decision turned to the issue of warrants, stating that “searches outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions” (*Katz v. U.S.*, 389 U.S. 347).

Although these cases were groundbreaking in their essence, neither resolved one of the most fundamental issues concerning domestic intelligence gathering, namely, the need for judicial oversight (primarily the issuance of
warrants) in situations where the President or executive officials have “asserted a special need for warrantless surveillance in national security cases” (Moore, 1003-1004). In fact, Justice White’s concurring opinion in Katz specifically stated in dicta that no warrant ought to be demanded when either the President or Attorney General has cited national security as the motivating cause necessitating such surveillance.

Congress responded to this the next year with the enactment of Title III of the 1968 Omnibus Crime Control and Safe Streets Act. Though drawn to meet the requirements elaborated in the Berger and Katz cases to protect individuals’ rights to privacy by establishing the requirement of either a judicial warrant, surveillance order, or elaborate executive finding in order to conduct surveillance, the statute pointedly provided that it was not meant to limit the Executive from conducting such intelligence gathering and surveillance as was necessary for national security:

Nothing contained in this chapter or in section 605 of the Communications 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. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. (Title III, Omnibus Crime Control Act, 18 U.S.C.A. § 2511)

With this law, Congress specifically acknowledged the existence of a variety of exemptions to the warrant requirement in the general sphere of national security; however, it was ambiguous regarding the full extent of these exceptions (Morgan, 122). It did suggest that there were five broad categories that were left unimpeded in regard to executive authority to engage in warrantless surveillance: to protect the nation against a foreign attack; to obtain foreign intelligence essential to national security; to provide counterintelligence pertaining to national security; to protect the U.S. government from overthrow; and to protect the U.S. government against clear and present dangers to its existence (Church, 106).

Within a few years, the Court heard a case involving the act and made a much more determinate ruling as to the nature of the Executive’s exception to the warrant requirement. In United States v. United States District Court for Eastern District of Michigan, commonly referred to as the Keith Case (in reference to the Judge petitioning the Court for a writ of mandamus), the Court specifically dealt with the legitimacy of the Executive to authorize
surveillance “in internal [or domestic] security matters without prior judicial approval” (U.S. v U.S. District Court, 407 U.S. 297). Speaking through Justice Powell, it first determined that the law itself was a clear expression, not of congressional prescription of executive power to exempt the warrant clause, but rather an expression of congressional neutrality in respect to such exceptions that might exist. Next, while recognizing that cases involving national security represent a sphere of Executive activity with a stronger “investigative duty,” the Court nevertheless maintained that these very same cases, when initiating domestic activity “often reflect a convergence of the First and Fourth Amendment values not present in cases of ‘ordinary’ crime…[moreover] given the difficulty in defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent” (U.S. v U.S. District Court, 407 U.S. 297). The balance of these competing interests, the Court ruled, in cases of domestic security clearly favors the Fourth Amendment freedoms, as they “cannot properly be guaranteed if domestic security surveillance may be conducted solely within the discretion of the executive branch” (U.S. v U.S. District Court, 407 U.S. 297). With the primary responsibilities of investigation and prosecution, the Executive is not a “neutral and disinterested magistrate,” and cannot be expected to act in a manner consistent with appropriate deference to the Fourth Amendment requirements (U.S. v U.S. District Court, 407 U.S. 297). Thus, the Court concluded, domestic surveillance requires appropriate and prior approval by the issuance of a judicial warrant. Justice Powell did, however, clearly point out that the decision did not address or even express an opinion as to the “issues which may be involved with respect to activities of foreign powers or their agents” (U.S. v U.S. District Court, 407 U.S. 297).

The collective result of these cases, then, divides the surveillance involving intelligence gathering into two different, though nevertheless colliding, spheres of constitutional responsibility. On the one side is foreign intelligence gathering, involving such concerns as national security and counterespionage, which is directed solely at the agents and/or collaborators of foreign countries. Such surveillance is not protected against by the U.S. Constitution nor does it require prior judicial oversight by the issuance of a warrant. On the other side is all of domestic intelligence gathering, as well as that foreign intelligence gathering which is not aimed at foreign agents and/or collaborators; constitutionally speaking, such surveillance is legitimate only if it is first authorized by a judicial warrant. On the face of it, such a distinction seems not only reasonably sanctioned by the Constitution, but also relatively simple to implement; however, in actuality, an unresolved issue prevents such a scheme from being
implemented unproblematically. The first is that this distinction is not nearly as clear-cut as it may first seem. The addition of ‘collaborator’ to the sphere of warrantless surveillance is a clear indication of the rather slippery slope involved in differentiating domestic and foreign intelligence concerns. As one of the initiators of major government abuses in surveillance, Tom Charles Huston noted:

The risk was that you would get people who would be susceptible to political considerations as opposed to national security considerations, or would construe political consideration to be national security considerations—to move from the kid with a bomb to the kid with a picket sign, and from the kid with the picket sign to the kid with the bumper sticker of the opposing candidate. And you just keep going down the line. (Johnson, *Season*, 82).

Inevitably, and as will be evidenced later, there will always exist wide disagreement as to what and who should qualify an individual as a domestic actor as opposed to a foreign agent or collaborator; when one takes up ideological purpose, it is often far too easy to be blinded by fervor in pursuit of those goals and fail to properly attend to such an ‘inconvenient’ distinction.

A Power Unchecked: COINTELPRO

The origin of the FBI’s counterintelligence program (COINTELPRO) can be traced back to as early as August 24, 1936, to a private meeting between the FBI Director J. Edgar Hoover and President Franklin D. Roosevelt, during which the President made known his apprehension over subversive communist and fascist elements within the United States (Theoharis, 67-68). Hoover was quick to latch on to the President’s fears and began a domestic intelligence gathering campaign that sowed the seeds for the top secret series of hard-hitting investigative and disruptive campaigns more widely known as COINTELPRO (Davis, 26). From its inception, COINTELPRO had been designed internally, and with ambiguous executive approval, for the express purpose of disrupting, discrediting, and neutralizing groups and organizations which, due to historic circumstances, were considered by government officials (particularly Hoover) to be subversive, dangerous, or threatening, whether ideologically, politically, or criminally, whether truly or merely apparently (Holt, 130).

To exacerbate this problem, COINTELPRO was a field-oriented set of operations that ran with virtually no outside supervision. The proverbial buck stopped with Hoover; beyond initial approval from the White House, no systematic executive oversight, or even interference of any sort, ever took place, neither from the Attorney General nor the Justice Department. Hoover and the assistant directors approved plans, and every individual involved knew that, ultimately, Hoover ran the program. In the end it was this sort of autonomy—from the laws, the government,
and morality in general—that allowed Hoover to construct a vast network that could, with near impunity, invade and
destroy the lives of countless Americans.

**Communist Party COINTELPRO**

The first COINTELPRO, informally authorized at the meeting of the National Security Council (NSC) on
March 8, 1956, was the culmination of anti-communist fears in the postwar period (Davis, 30-32). Having already
employed 1,600 special agents and 5,000 paid informants to track and disrupt the U.S. Communist party, Hoover
sought presidential approval for “penetration of the Party at all levels; use of various techniques to keep the Party off
balance and disillusion individual communists concerning communist ideology” (Wall, 40). In fourteen years of
operation, the COINTELPRO directed at the Communist Party initiated over 1,388 actions, successfully achieved at
least 222 known results, and all but decimated the Communist party in the U.S. In 1956, it had around 22,000
members; by 1971, this figure was closer to 3,000, and much of that number consisted of inactive members and FBI
informants (Davis, 51).

In a business that was described by top FBI officials as “imbued with war psychology,” legality often fails
to register as a legitimate concern (Church, 144). The Communist Party COINTELPRO was begun as part of a
larger struggle against communism throughout the world in order to protect the security of the U.S., and though it
was largely a matter of ideology, the attitudes of top governmental officials certainly spurred an “action-oriented
group of people” in the FBI into battle against an uncertain enemy (Church, 146).

**Black Nationalist Hate Group COINTELPRO**

What began with the Communist Party COINTELPRO spread to groups such as the White Hate Groups and
the New Left, and culminated with the Black Nationalist Hate Group COINTELPRO. With the backdrop of a few
extremist black groups and racial riots that cost at least 225 deaths, 4,000 injuries, and over a billion dollars in
property damage, President Johnson wanted answers, and with preliminary investigations revealing that neither were
any of these groups under any form of foreign influence nor were the riots organized on a nation-wide basis, the
President wanted more direct studies (Davis, 100; Church, 83). After the Detroit riots in 1967, Hoover himself sent
out a memorandum initiating a COINTELPRO with the aim to “expose, disrupt, misdirect or otherwise neutralize
the activities of black nationalist hate type organizations” (Blackstock, 14). Given the fact that this project was
beyond the scope of presidential authorization, an addendum was included which stated, “you are cautioned that the nature of this new endeavor is such that under no circumstances should the existence of the program be made known outside the Bureau” (Church, 147). A counterintelligence program aimed at groups that had been exonerated from suspicion of foreign ties was ironic enough, but the makeup of the list that specified which groups were to be neutralized—from the Congress on Racial Equality to the Student Non-violent Coordinating Committee and the Southern Leadership Conference—was beyond belief (Church, 69-70).

Less than a year after its creation, the Black Nationalists Hate Group COINTELPRO had double the entire size of the FBI counterintelligence program, running between 5,000 and 10,000 active cases on matters of race at any given time (Wall, 112). It signaled the full embrace of Hoover’s statement: “The Negro youth and moderate must be made to understand that if they succumb to revolutionary teaching, they will be dead revolutionaries” (Davis, 103). One special agent recalled that “the appalling racism of the FBI on every level became glaringly apparent” during this time period; nevertheless, no such sentiments could have had a “direct bearing on the investigations or the basic thrust of this COINTELPRO. Hoover’s word was the law” (Davis, 106).

This time the FBI did not merely sit idly by while violence occurred, rather the FBI incited the violence. Pitting two groups, the Black Panther Party (BPP) and the United Slaves Incorporated (US), which are both known for their militancy (Hoover had referred to the Panthers as the “greatest single threat to the internal security of the country”), against one another, the FBI used anonymous phone calls, mailings, and informants to promote division and confrontation between the two groups (Wall, 123). Tensions mounted, shootings and street violence increased, and internal memos state unequivocally that “a substantial amount of the unrest is directly attributable to this program…in view of the recent killings[s more operations are] being considered in the hopes that it will assist in the continuance of the rift between BPP and US” (Davis, 110). Neither the recognition of their close association with violence and crime, nor even the realization that they directly provoked such activities, would curb FBI behavior in these spheres of influence.

Indeed it seemed only to spur them on to most ambitious goals; “all its available resources” were brought to bear on “general racial conditions” in the country (Church, 71). In March of 1968, new, long-range objectives were fashioned, which included such directives as preventing the “coalition of militant black nationalist groups,” the rise
of a “messiah” who could “unify and electrify” the movement, and groups and leaders from gaining “respectability” by discrediting them to the “responsible Negro community” (Blackstock, 22-23).

Highlighting the absurdity of these goals was one of the most insidious and shameful dealings in which the FBI was engaged in under the auspices of COINTELPRO: its investigation of Dr. Martin Luther King Jr. throughout the 1960’s. Although begun under the Communist Party COINTELPRO in the late 1950’s, the King investigation continued long after he was cleared of any communist ties, using the justification that “Dr. King might ‘abandon’ his adherence to nonviolence” (Church, 173). Its objective was clear—to take “King off his pedestal and reduce him completely in influence” (Wise, 302). According to internal documents, King was “the most dangerous Negro of the future in this nation” (Church, 250). The surveillance brought together every weapon then in the FBI’s extensive arsenal, beginning with wiretaps and secret microphone surveillance in nearly every location to which King could be thought to have traveled to, ranging from his home to the headquarters of the Southern Christian Leadership Conference in both Atlanta and New York, to innumerable motels and hotels across the country; one agent on the case noted that at least “5,000 of King’s calls were intercepted over a period of years…the surveillances was massive and complete. He couldn’t wiggle” (Davis, 42). The FBI attempted and often succeeded in persuading groups to withhold financial and political support to King, as well as to the various organizations with which he was involved; in fact, they even used Cardinal Spellman of New York to attempt to dissuade the Pope from meeting with King (Davis, 44). The FBI attempted to prevent King from receiving other awards and prestigious honors such as the Nobel Peace Prize and various honorary degrees (Johnson, “Congressional,” 14). Anonymous letters meant to blackmail King were sent to his home and went so far as to try to convince King to take his own life. After mailing a letter and semi-audible tape supposedly recorded during a romantic liaison, the FBI followed up with a second letter 34 days before his Nobel Prize acceptance:

King, there is only one thing left for you to do. You know what it is. You have just 34 days in which to do it. (The exact number has been selected for a specific reason.) It has a definite practical significance. You are done. There is but one way out for you. You better take it before your filthy, abnormal fraudulent self is bared to the nation. (Wise, 305)

The harassment did not even end with his death. The FBI went so far as to construct plans to disrupt the creation of a national holiday on the date of his birthday (Johnson, 13-14).
Perhaps the most disturbing part of the King affair was the lack of concern for legality, constitutionality, and morality by the FBI. Not only did King have no ties to the Communist Party, not only did he eschew all forms of violence in his protests, but not once did the FBI, according to Congressional testimony, have any evidence whatsoever that would allow them to be suspicious that King “was about to or had committed a crime…foment violence…or ever participate in violence” (Johnson, “Congressional,” 14). By its termination in 1971, the Black Hate Groups COINTELPRO had engaged in what one of the directors of the program, William Sullivan, called a “rough, tough, dirty business, and dangerous” (Davis, 124). Ironically, Sullivan failed to grasp in his assessment why this operation was in truth so rough, tough, dirty and dangerous. Numerous individuals had been killed as a direct result of FBI actions. Non-public, damaging information had been made known to the media on countless occasions, decimating groups and individuals in the public’s eye, thus ultimately, too many lies, threats, and intimidations were made in the attempt to destroy U.S. citizens, personally, economically, and even physically.

Revelations of Abuse: Church Committee

Investigations into the FBI’s domestic intelligence abuses culminated in 1976 with the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities’ (the Church Committee) report on the intelligence committee. Although prior Attorney General, congressional, and media reports did reveal some information, most were “brief FBI-prepared summaries,” and none were as thorough, deeply probing, nor had access to as much information as the Church Committee (Church, 131). Its report determined that during COINTELPRO:

- approximately 500,000 files on individuals and groups had been opened which could include information on numerous people only obliquely associated with them (47);
- 740,000 investigations of ‘subversive matters’ had been undertaken, against such groups as writers (John Steinbeck), universities, churches, and political parties (167-168);
- the “abusive techniques used by the FBI” violated state and federal laws prohibiting “mail fraud, wire fraud, incitement to violence, and extortion” and also “infringed the rights of countless Americans under the Fourth Amendment protections;” these often occurred without external approval (139, 62);
- “when officials did assume, or were told, that a program was illegal, they still permitted it to continue” (138);
- massive amounts of information were accumulated on “lawful activity and law-abiding citizens…not at all related to law enforcement or the prevention of violence” (68);
- the FBI deliberately exaggerated the threat of Communist influence in order to justify investigating various individuals and groups (49);
- its standard for intelligence collection was overly broad, including individuals and groups not suspected of criminal activity nor relevant to any legitimate governmental interest (50, 165);
- the FBI often “fails to disclose candidly their programs and practices to their own General Counsels, and to Attorneys General, Presidents and Congress” (138);
• statutory and constitutional controls and procedures on surveillance and related activities have been insufficient (183).

The FBI admittedly engaged in over 2,200 separate operations under the COINTELPRO heading, many of them coupled directly with such illegalities as the warrantless phone taps, 2,305 admitted, and bugs, 697 admitted, and mail openings, 57,846 admitted (Wall, 303). These activities constituted a full 19 percent of the FBI’s investigations; moreover, only 3 percent of the cases investigated were even referred on to authorities for prosecution, and only 2 percent were believed to have prevented any threat or violence (Morgan, 55). The FBI had clearly crossed too many constitutional, statutory, and ethical lines during its COINTELPRO investigation, resulting in the penetration and disruption of countless innocent American lives.

When the question of how and why this was possible is posed, a plethora of answers present themselves. The FBI was an agency operating with minimal oversight from both within the Executive Branch and without. Congress was not involved in oversight of the intelligence community in any relevant sense. The Supreme Court’s directives were vague enough to be interpreted as sanctions for nearly any action remotely connected with a foreign concern. The United States was preoccupied with the Cold War and the possible subversion Communist and Communist-affiliated groups could reap at home. In the midst of this accountability nightmare, a director of the FBI emerged with the capacity to exact the highest and most unquestioning standards of loyalty, even if it meant engaging in illegal activities. With this political climate, this structural organization of the FBI in regards to oversight and accountability, this ambiguity between foreign and domestic actors, and these commanding figures, abuse was entirely foreseeable if not actually inevitable. In the wake of the Church Committee’s report, steps were finally taken to correct some of these mistakes. One of the clearest needs was a clarification of the “administrative, legislative, and judicial guidelines for…[domestic] intelligence operations,” and in this regard the Foreign Intelligence Surveillance Act was implemented in 1978 (Elliff, 228).

**The Road to FISA**

The Foreign Intelligence Surveillance Act of 1978 (FISA) was implemented in order to regulate warrantless electronic surveillance for intelligence purposes. The immediate impetus for the passage of FISA was the Church Committee’s report that uncovered the abuse of unchecked power by the Executive Branch and the FBI. However, FISA was the culmination of a plethora of different actions that began well before the Church Committee was
formed. Barbara Stolz claims that FISA was the result of a “nexus of contextual factors,” that occurred at the convergence of several concerns (277).

The political and legal concerns were far-reaching. The actions of the Judiciary have already been discussed extensively and will not be revisited. Yet, it was not just the Judiciary that had been trying to interpret the government’s power to pursue foreign intelligence domestically. The Legislative Branch and the Executive Branch have been addressing wiretaps and surveillance for decades. Sometimes the branches acted independently of each other, while in other instances the actions of one branch were a direct reaction to the actions of another. In order to fully understand FISA, it must be viewed in light of the history that preceded it. It is in this context that it becomes clear why the statutory framework that resulted from FISA involves all three branches of government. The following discussion will explore the actions of the Executive and Legislative Branch that culminated in the passage of legislation to regulate surveillance for intelligence purposes. The legislative and executive history will augment the discussion on the judiciary to provide a complete framework in which to understand the passage of FISA in 1978.

**Legislative History Leading to FISA**

From 1950 to 1974, almost 200 bills were introduced to increase the accountability of the intelligence community to Congress. Not a single one passed. The first blow to this intelligence community armor of absolute authority finally came in 1974 with the passage of the Hughes-Ryan Act (Clarke and Neveleff, 494). This act did not, however, address the issue of wiretaps, and only began taking steps towards regulating wiretaps in 1968 with the Omnibus Crime Control and Safe Streets Act in 1968. Yet, as discussed earlier, this statute made a point of specifically disclaiming any intention to affect the constitutional powers of the President in foreign affairs and intelligence matters (Cinquegrana).

It was not until 1976 that a bill serving as the precursor to FISA emerged in the Senate. Senator Kennedy introduced a bill designed to regulate electronic surveillance in the national security domain. This bill specifically repealed the provision of the 1968 Omnibus Act that addressed the President’s constitutional authority in this area. The bill intended to eliminate, or at the least limit, the President’s authority to order searches without a warrant. The bill created a warrant requirement in order to intercept not only domestic communications, but also international
communication to or from targeted Americans in the United States. The provisions that allowed for the targeting of Americans who had not violated any federal criminal law were the most contentious issues in the hearings on this bill (Cinquegrana).

The House also considered legislation during this period. In 1976, an alternative bill was introduced which was a companion to the Kennedy bill, but offered greater support to the bill offered by President Ford. In the end, none of this legislation passed during the 94th Congress. The session ended before the full Senate had an opportunity to vote on the bill. There were also differences that remained between the House and Senate and between the White House and Congress (Stolz, 279). While no legislation was passed, what began in the 94th Congress would finally bear fruit when the 95th Congress convened.

**Executive History Leading to FISA**

In 1940, President Roosevelt acted unilaterally by informing Attorney General (AG) Jackson that listening devices were to be used in situations where “grave matters involving [the] defense of the nation” may be involved. However, he also instructed Jackson to limit this surveillance to aliens as much possible (Cinquegrana). President Truman took FDR’s actions a step further in approving broader use of electronic surveillance in matters that involved domestic security. In the period between World War II and 1978, the office of the Presidency claimed an inherent right to authorize electronic surveillance in areas concerning national security. Certain assumptions regarding Presidential power were fundamental to this tenet of authorizing searches without a warrant in the realm of national security. One of the overriding assumptions was that the power to conduct foreign affairs was superior to the restriction on warrantless searches imposed by the Fourth Amendment of the Constitution. These attitudes were finally toned down in the immediate aftermath of the Church Committee.

On March 23, 1976, President Ford sent the Senate a bill to regulate electronic surveillance. The bill drew upon the Supreme Court’s suggestions in the *Keith* case that Congress could provide specialized warrants to account for the different governmental and private interests involved. The bill suggested that upon a finding of probable cause, a warrant could be issued to intercept wire or oral communication if the target was an agent of a foreign power and was engaged in clandestine activities (Cinquegrana). However, Ford was unwilling to relinquish all authority in this arena. His proposal allowed the president to retain power to authorize surveillance in circumstances
outside the scope of the bill and where such surveillance could be deemed necessary for national defense. The bill remained in Congress for the next two years. There was substantial discussion that focused on the question of reserved presidential authority and whether a “criminal standard” should apply to Americans before surveillance could be initiated. President Ford left office without the realization of this bill, yet the discussion the bill created and some of the ideas it introduced would be present in the eventual law passed in 1978.

Passage of FISA

The path that led to the Foreign Intelligence Surveillance Act spans several decades, but these events accelerated in the years immediately prior to 1978. Both the Executive Branch and Congress made failed attempts to implement similar legislation in 1976. In 1977, the reigns of the executive branch passed from President Ford and the Republican Party to President Carter and the Democrats. On May 18, the president’s proposal for legislation on electronic surveillance was announced. The proposal was drafted by an interagency committee chaired by AG Griffin Bell. The Carter legislation overcame one of the major objections by Congress to the Ford bill. The bill made no overt reservation to inherent presidential power. Senators voiced their appreciation for the administration’s more tempered stance on presidential authority. Within a few weeks the bill was introduced in both the House and Senate (Oseth, 110).

Senator Kennedy introduced the Foreign Intelligence Surveillance Act of 1978 (S. 1556) in the Senate on the same day the President announced his proposal. Just as in 1976, co-sponsorship of the bill was bipartisan. The chamber as a whole passed the bill on April 20, 1978 (Stolz, 280). The vote was a resounding ninety-five to one (Smist, 101). Although the bill had made it through the Senate, it had still not passed the House where it faced some serious opposition.

The House Permanent Select Committee on Intelligence (HPSCI) examined alternative bills and conducted several hearings (Cinquegrana). Their recommendation was that the House should enact the House version of the Kennedy bill. The discussions that occurred concerning the bill illustrated the various positions of opponents to the proposed legislation. Some representatives did not want to see the diminution of what they regarded as the President’s inherent authority to permit warrantless searches in matters concerning the nation’s security. Others opposed the legislation because they believed that probable cause must exist showing that a crime had been
committed before any search could take place (Stolz, 280-81). Despite these objections, the bill passed the House on September 7, 1978. The two chambers worked out their differences in conference and presented the President with the bill on October 16, 1978.

The actions and events of several decades culminated on October 25, 1978, when President Carter signed the bill into law (Stolz 281). In his public statement at the signing, President Carter recognized the unprecedented nature of the bill. He stated that the new law would introduce clarity where there was once contention. He did not address the fact that he had bargained away a power that his predecessors viewed as inherent in the position (Oseth 111). Not only was the act supported by Congress and the White House, but also by various civil liberties groups and national security organizations (Stolz 281). The legislation achieved a delicate balance between the executive and legislative branch.

**The Foreign Intelligence Surveillance Act of 1978**

The passage of this act was an historic occasion. It represented a major concession on the part of the President (Oseth, 64). The act also finally helped to clarify a picture muddied by varying interpretations from the Executive, Legislative, and Judicial Branches. Where once there were no guidelines, FISA implemented a framework in which multiple prerequisites had to be satisfied in order to undertake any action in the foreign intelligence surveillance arena. FISA also established the Office of Intelligence Policy and Review (OIPR) within the Department of Justice (DOJ) to help carry out the law. OIPR prepares FISA applications and also represents the United States before the FISA court (Stolz, 282).

**Electronic Surveillance**

FISA radically transformed the way in which electronic surveillance for national security purposes is both approved and conducted. However, it is important to realize that the level of scrutiny varies depending on the parties subject to surveillance, and members of Congress, as well as civil liberties groups, have made their feelings quite clear that there should be greater protections for United States citizens and permanent residents. These concerns were reflected in the legislation which created a higher bar for monitoring U.S. persons.

The president, acting through the Attorney General may authorize electronic surveillance without a court order for up to one year when the parties involved are foreign powers. However, the Attorney General has to certify in writing and under oath that electronic surveillance is indeed only directed at communications between or among foreign powers. The key
provision here is that there must exist no “substantial likelihood” of acquiring the communications of a U.S. person (50 USC §§ 1802 (a)(1)(A-B)). There are much more stringent regulations in place for the surveillance of a suspected agent of a foreign power, which may well be a U.S. person.

Similar to the application for surveillance of foreign powers, the Attorney General must approve the proposed surveillance. However, in the case of an agent of a foreign power, an application must be submitted to the Foreign Intelligence Surveillance Court (FISC) and the list of requirements that the Attorney General must certify is much more extensive. In order to file an application with the FISC, the application must include, if known, the identity of the target of the surveillance, or at least provide a description of the target (50 USC § 1804 (a)(3)). The application must also include a statement of the facts that demonstrates that the target is in fact either a foreign power or an agent of a foreign power and that facilities being monitored are being used, or are about to be used, by a foreign power or an agent thereof (50 USC § 1804 (a)(4)). One important requirement that must be provided for is a statement of the minimization procedures that will be employed (50 USC § 1804 (a)(5)). Minimization procedures reduce the risk that information obtained during surveillance will be improperly used or distributed. A FISA warrant cannot be used to fish for information in the hopes of running across something. One of the requirements for the issuance of a warrant is a detailed description of the nature of the information being sought as well as the type of communications or activities that will be subjected to surveillance (50 USC § 1804 (a)(6)).

The next item required by FISA has proven to be the most contentious in the current debate surrounding FISC warrant applications.

FISA requires an Executive Branch official in the field of national security or defense who has been appointed by the President and approved by the Senate to certify that the information being pursued is in fact foreign intelligence information and that the “significant purpose” of the surveillance is to obtain foreign intelligence. (50 USC §§ 1804 (a)(7)(A-B)). When FISA was originally passed, this requirement stated that “the purpose” of the surveillance was to gather foreign intelligence. While on the surface this change made by the PATRIOT Act may seem slight, replacing these two words has radically changed how the Executive Branch and the Foreign Intelligence Surveillance Court of Review (FISCR) interpret the act. FISA also requires that this same Executive Branch official certify that the information being pursued could not be obtained by normal investigative techniques (50 USC §§ 1804 (a)(7)(C)). This requirement is vital since the use of a FISA warrant circumvents the traditional Fourth Amendment requirements for search and seizure. If all of the requirements
stipulated by FISA in 50 USC § 1804 are met, then an application for electronic surveillance is presented to the FISC for a decision.

**Physical Searches**

When FISA was originally passed in 1978, it included no requirements for physical searches. Warrant-less physical searches in the foreign intelligence arena continued to be under the sole discretion of the Executive Branch (Malooly, 412). While there was no explicit language pertaining to physical searches, the Carter administration maintained that FISC along with the office of the President had concomitant authority to approve physical searches for intelligence purposes (Clarke and Neveleff, 498). The Carter administration, however, rarely appealed to FISC in order to conduct a physical search, submitting only three applications. Despite this rare utilization of FISC in physical searches, the administration’s actions allowed for some judicial participation. Yet not everyone believed there needed to be any judicial involvement in this area. Both the House and Senate Intelligence Committees expressed concern and had reservations about FISC venturing into physical searches. FISC itself was unsure about its proper role in this area and asked the Clerk of the Court to prepare a memorandum on the subject. The memo concluded that neither the statutory language nor the legislative history gave any suggestion that FISC has power to authorize anything other than electronic surveillance (Cinquegrana). This attitude was shared by the incoming administration.

The Reagan administration was unreceptive of FISA from the start. Admiral Stansfield Turner, Director of Central Intelligence (DCI) under President Carter, was told that he would not be reappointed DCI because of his support for the passage of FISA (Turner, 161). In fact, the Reagan administration originally planned to introduce a bill on Inauguration Day to repeal FISA. The administration strongly objected to the fact that they had to go to FISC for wiretap approvals (Turner, 161). This consternation was also extended to any FISC involvement with physical searches. The administration maintained that only the president and the Attorney General, by delegation, had the constitutional authority to approve physical searches for intelligence purposes (Clarke and Neveleff, 498). President Reagan was about to take two separate actions to ensure that FISC no longer participated in physical searches.

In the spring of 1981, the Department of Justice under William French Smith, Reagan’s first Attorney General, submitted another application to the FISC for authorization to conduct a warrantless physical search to gather foreign intelligence. However, this application was never meant to be approved. The Department of Justice included with the
request a memo of law that argued that FISC had no jurisdiction to grant such an order, and it requested that the application be rejected. FISC concurred with this, and on June 11, 1981, issued an opinion stating that the court does not have and never had the authority to approve physical searches (Cinquegrana). President Reagan also issued Executive Order (EO) 12,333 in response to this issue. The Executive Order held that the Attorney General had the power to approve any technique that would normally require a warrant for law enforcement, as long as it is directed against either a foreign power or an agent of a foreign power (Malooly, 413).

In 1982, the Senate Select Committee on Intelligence (SSCI) began to backtrack on their earlier stance. They recommended that “consideration be given to the possibility of amending [FISA]… to provide a statutory basis for physical searches in the United States for intelligence purposes” (Clarke and Neveleff, 499). Clarke and Neveleff claim that subjecting physical searches to the same requirements of electronic surveillance would not only alleviate some of the apprehension about executive oversight of the process, but it could also bolster the morale of those conducting the surveillance to know that their actions were lawful (499). These arguments were not compelling in 1982, and the issue remained unresolved for more than a decade. It would take an external threat to the process to finally bring physical searches within the framework of FISA.

This threat and the impetus for change appeared in the person of Aldrich Ames. On October 10, 1993, FBI agents broke into Ames’ house.

The team of specialists proceeded to methodically examine the contents of the entire house… the team left, making sure that everything was returned to its proper place. The owners of the house would never know that this search had taken place, unless the FBI decided to tell them. (Malooly, 411)

It was this search of Ames’ home that confirmed the suspicions of the task force investigating him. This search produced evidence of Ames’ ties with the Soviet Union’s KGB. While the FBI should have been breathing a sigh of relief, they were soon worried that all of the crucial evidence they just obtained may be jeopardized. Ames’ attorney was planning to challenge the constitutionality of the search. In fact, the courts had not addressed this issue; thus, there was not any judicial or legislative guidance on which the FBI could feel confident in its methods. Fortunately, for the government, this judicial challenge never materialized. Ames, against the wishes of his attorney, chose to plead guilty in exchange for leniency towards his wife (Malooly, 411-412). This case illustrates the tenuous position of warrantless physical searches. Congress decided it was not going to wait for a judicial ruling against these searches before it acted. In 1994, Congress amended FISA
to include physical searches for foreign intelligence purposes. The requirements to receive a warrant for a physical search from FISC mirror those required for electronic surveillance (50 USC §§ 1822-1823).

One aspect of FISA orders that has yet to be discussed is the separate standard for emergency orders. If an emergency situation exists with respect to either electronic surveillance or physical searches, the Attorney General is allowed to authorize surveillance after informing a FISC judge that such an authorization is taking place. The AG then has seventy-two hours in which to submit the typical FISA application. If the application is denied by FISC, then the surveillance is terminated and no information obtained from it is admissible in any forum (50 USC § 1805 (f); 50 USC § 1824 (e)).

In addition to electronic surveillance and physical searches, FISA allows the FBI to submit an application for an order requiring the production of books, records, papers, documents, and other items for an investigation aimed at gathering foreign intelligence information (50 USC § 1861 (a)(1)). Applications for these items are also made to FISC. If FISC issues an order, the fact that the investigation concerns foreign intelligence is not disclosed to any recipient required to produce documents (50 USC § 1861 (c)(2)). In addition, anyone required to produce these “tangible things” is not allowed to tell anyone else that such a request was made (50 USC § 1861 (d)).

**The Foreign Intelligence Surveillance Court and Court of Review**

Due to the sensitive nature of the material included in any warrant for either electronic or physical surveillance, Congress created a special court to rule on these applications.

**The Courts**

Judges to both the FISC and FISCR are appointed by the Chief Justice of the Supreme Court. FISA, as originally passed in 1978, is comprised of seven judges.¹ The judges are district court judges and must come from at least seven different judicial circuits, with no fewer than three residing within twenty miles of Washington, D.C.² (50 USC § 1803 (a)). FISCR consists of three judges, of which one is designated the presiding judge. FISCR judges may either come from district courts or courts of appeals (50 USC § 1803 (b)). Judges for both courts are appointed to serve for a maximum of seven years and are not eligible for redesignation (50 USC § 1803 (d)). In order to protect the sensitive national security information being presented in these applications, proceedings are conducted under strict physical security measures (Cinquegrana).

---

¹ The Patriot Act has increased this number to eleven.
² This clause regulating distance from D.C. was added by the PATRIOT Act.
FISC meets in a special room in the Department of Justice, and there is at least one judge on call twenty-four hours a day for emergencies (Turner, 156).

All applications prepared along the guidelines of § 1804, discussed above, are presented to FISC, which will decide whether or not a warrant is to be prepared. If the judge finds that all of the requirements of § 1804 have been met, then he will approve the application and grant the warrant (50 USC § 1805). If a judge should choose not to approve an application, he or she shall provide a written statement outlining each reason for his decision (50 USC § 1803 (a)). The petitioner then has the option to appeal the decision to FISCR. This court has the opportunity to either overrule FISC or hold their decision to be correct. If FISCR does not overrule FISC and also denies the application, it also has to provide a written statement of the reasons for its decision (50 USC § 1803 (b)). The Executive Branch’s only remaining recourse if both courts reject an application is to appeal to the Supreme Court (50 USC § 1803 (b)).

**Track Record**

From the time that FISA implementation began in 1979 through the end of 2002, there were 15,247 applications for warrants. In this twenty-four year period, only two applications were denied by FISC. The application that the Reagan administration requested to be denied has already been discussed. The only other application that has been denied was overturned by FISCR. Professor Jonathan Turley, a former NSA staffer, stated,

> When you enter the FISA chamber you’re struck by the absence of procedures or protocol normally associated with a legal proceeding… If the FISA court ever turned down one of your warrants, it would be like a notary refusing to sign off on a lease agreement” (Malooly, 415).

During the debate over FISA in the House, skeptics questioned the validity of a judicial review process. They argued that judges are inclined to respect and defer to the rationale of national security surveillance, and would be unlikely to act as a substantial check on the desires of the Executive Branch (Oseth, 111). Many believe that FISA is a complex set of procedures designed only to give the illusion of protecting individual rights while it actually only serves to cover up what is really a rubber stamp for government requests (Malooly, 415).

Despite the misgivings of FISA’s critics, it can be argued that because of all of the requirements put forth by FISA, the applications are well thought out and scrubbed before they ever make it to the court (Cinquegrana). Perhaps there were many more searches that would have occurred had FISA not been in place. In his book, *Secrecy and Democracy*, DCI

---

3 This number is taken from compiling the number of warrants reported in the Attorney General’s annual public report on FISA.
Turner relates the careful thought he put into pursuing a warrant application because he was not sure whether the situation met the guidelines of FISA. He agonized over whether he could prove that the U.S. person under surveillance was an agent of a foreign power. He said that FISA forced him to think deeply about the importance to the country of invading an individual’s privacy. Even if he decided to go forward, he still had to convince the Attorney General. He states that the process intended to protect the suspect also protected the intelligence community from “being carried away by either an excess of zeal or bad judgment” (Turner, 155-56). Proponents of FISA will point to this type of consideration as evidence that FISA is in fact an effective tool to protect civil liberties. In response to the argument that judges would defer to the Executive in matters of national security, FISC judge Royce Lamberth, said, “I have a grave and extraordinary responsibility to protect the legitimate rights of parties who are not represented before the court… I don’t take that lightly, nor have I seen any evidence that any other judge does” (Malooly, 416). However, there are very few individuals who really know what happens within the FISC chamber or even how the process truly operates. Due to the secrecy that surrounds the court, it is difficult to determine whether the 99.997% application approval rating is evidence that FISC has become a captive of the national security establishment or whether only legitimate applications make it past the rigorous requirements of FISA.

**Shrouded in Secrecy**

It is clear that the information involved in FISA proceedings is sensitive in nature. The protection of this information is needed not only for national security purposes, but also to prevent information about anyone under surveillance from being leaked. The records of all proceedings, including applications and orders, are kept under security measures established by the Chief Justice with the advice of the Attorney General and the DCI (50 USC § 1803 (c)). The only parties that ever gain a glimpse into the proceedings of the court are representatives from the Department of Justice and the FISC judges themselves. Although the actual execution of electronic surveillance involves communications companies, they must maintain information about such actions under security procedures approved by the Attorney General and the DCI (50 USC § 1802 (a)(4)(B)).

In addition to these security measures, very little information about the court is ever publicly released. The only publicly available information is contained in a letter sent by the Attorney General every April to the Administrative Office of the United States Court and to Congress. This letter simply states the number of applications sought over the past calendar year and how many of these were granted, modified, or denied (50 USC §§ 1807 (a-b)). The AG is required to provide more
information to HPSCI and SSCI on a semiannual basis. Concerning electronic surveillance, these reports include the number of times that information acquired from a warrant was used for law enforcement purposes as well as the number of times information is used in a criminal trial (50 USC §§ 1808 (a)(2)(A-B)). In the first five years of FISA implementation, both HPSCI and SSCI reported back to their full chambers with an analysis on FISA actions over the last year. Each committee had the opportunity to offer recommendations as to whether the legislation should be amended, repealed, or left alone (50 USC §§ 1808 (b)). Unfortunately, this requirement ended two decades ago. The AG must also provide information on physical searches on a semiannual basis. On a semiannual basis the AG is to “fully inform” both HPSCI and SSCI (50 USC § 1826 (a)). He also provides both of those committees, as well as the Judiciary committee, of each chamber with a report indicating the total number of applications for physical searches, whether these searches were granted, modified, or denied, and finally how many of those searches involved U.S. persons. However, all of this information is available to a very few individuals, and what is publicly available pales in comparison.

The “Wall” or Lack Thereof

The case of United States v. Truong Dinh Hung was considered prior to, but affirmed after, the enactment of FISA. The Court of Appeals for the Fourth Circuit made a clear distinction between information used for foreign surveillance and that used for law enforcement purposes. The United States was conducting foreign intelligence surveillance against Truong and eventually used information obtained during surveillance to prosecute him. The Court held that information obtained after the primary purpose of the surveillance had changed from foreign intelligence to law enforcement was not admissible at his trial. They held that once the primary purpose had shifted, the government had the burden of satisfying the requirements of the Fourth Amendment (“Who’s Listening”, 306-307). This strict partition between foreign intelligence and law enforcement is known as the “wall.” The idea that the two should be separated was the prevailing belief until the administration of George W. Bush. In fact, in 1995, Attorney General Janet Reno issued guidelines to ensure that this separation occurred. However, in 2002, Attorney General John Ashcroft deconstructed the wall by issuing his own guidelines in radical opposition to the 1995 guidelines and what had long been the prevailing thought on the matter.

Primary Purpose

As FISA was originally enacted in 1978, § 1804 (a)(7)(B) stated, “that the primary purpose of the surveillance is to obtain foreign information.” It was this language that the court used in Truong to establish the primary purpose test. During
the 1980’s, federal courts continued to interpret FISA as prohibiting electronic surveillance if the primary purpose was not the gathering of foreign intelligence (“Recent Cases”, 2247). On July 19, 1995, Janet Reno issued a memorandum outlining procedures to maintain the “wall.” As stated in the memo, “the purpose of these procedures is to ensure that [foreign intelligence (FI) and foreign counterintelligence (FCI)] investigations are conducted lawfully, and that the Department’s criminal and intelligence/counterintelligence functions are properly coordinated” (Reno). The guidelines are very specific in how the FBI should communicate with both the Criminal Division (CRM) and OIPR.

The guidelines establish a step-by-step process through which FI or FCI information can be utilized in a criminal investigation. If it appears during the course of a FISC approved investigation that a federal crime is being committed, the FBI and OIPR each have to independently notify the Criminal Division. Before the Criminal Division can consult with the FBI about this information, it must notify OIPR of its intention to do so. Furthermore, the FBI may not contact a U.S. Attorney’s Office without the approval of both CRM and OIPR. The guidelines require the FBI to “maintain a log of all contacts with the Criminal Division, noting the time and participants involved in any contact, and briefly summarizing any communication” (Reno). While the Criminal Division may give guidance to the FBI on preserving the option of a criminal prosecution, it shall not “instruct the FBI on the operation, continuation, or expansion of FISA electronic surveillance or physical searches” (Reno). In addition, if a FISA renewal application is pending, OIPR will inform FISC of any contacts between the FBI, the Criminal Division, and the U.S. Attorney’s Office, in order to keep the court informed of any law enforcement facets of the investigation. These guidelines were further supported by the Department of Justice in a memo issued in 2000.

A working group consisting of senior officials from the Criminal Division, FBI, and OIPR made recommendations as to how the Department of Justice should handle intelligence investigations. The resulting memo that outlined some of these recommendations stated, “there is unanimity within the working group that the 1995 Procedures set forth the correct substantive standard with respect to notification to the Criminal Division” (Gindler and Schwartz). The memo also made some suggestions as to further regulating intelligence sharing between FBI and the Criminal Division. As a result of this memo, the Attorney General adopted additional measures to ensure that communications between FBI and the Criminal Division remain within the scope of the law (Thompson). Less than two years later, these carefully studied regulations would be swept away under the force of the PATRIOT Act.
**Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism**

Act (USA PATRIOT Act) of 2001

The PATRIOT ACT is no different than previous orders and laws that stripped away the Constitutional rights of American citizens. Though the legislation may have been passed with the best of intentions – namely, protection of the American people and its homeland from terrorism- it fails to protect the American people from its own government. Some would argue that a certain amount of trust should be placed in the government, a Hamiltonian view that the masses should rely on the decisions of the elite because they will work in the interest of the whole. However, as previously exemplified, the rights of the masses during times of panic and warfare are often shelved by administrations under the guises of “protection” and the necessity of “times of war.” The USA PATRIOT Act is no exception to the pattern.

**The Passing of the PATRIOT Act**

The tragic events of September 11th, 2001 not only destroyed many innocent lives but also threw the balance of power in favor of the Executive and Justice Department. In no way should the victims of 9/11 and the ensuing tragedy ever be undermined. However, the events on that fateful day had much to do with the passing of the Act. In congressional records of the floor proceedings for both the House and Senate the day the PATRIOT Act was brought forth for approval, there was a consistent mention of how the Act was pertinent towards correcting the mistakes of 9/11 by introducing legislation that would correct those wrongs.

Moreover, barely a month after September 11, 2001, the country was in a state of heightened awareness because of an anthrax scare across the nation. Thus, the writers and proponents of the Act utilized the present fear to both influence the provisions written and incite support on the Hill. Immediately after the Act was passed in October of 2001, Sen. Orrin Hatch (R-UT) stated that the majority of Americans would not see the law as an erosion of civil rights: “I don’t know anybody in this country who’s afraid of their law enforcement people at this time. They’re afraid of terrorism” (Lawrence, 5). Further, the name of the Act incites an obligatory response. The Act is associated with “patriotism” for the United States. Voting “nay” would mean a vote against patriotism.
Using terrorism and the existent atmosphere, the Act was rushed through by its proponents, and as a result lacks the possibilities for oversight and checks from one branch to the next. Originally proposed in the Senate on October 11, 2001, it took no more than two weeks for the Act to be approved in the House of Representatives by a vote of 357 to 66 on October 24th. Express mailed to the Senate, the Act then passed with little controversy or debate by a vote of 98 to 1. As the very first Senator to take the floor when the USA PATRIOT Act was debated on October 25, 2003, Senator Leahy (D-VT) declared in his opening statement, “We do want to have discussion of this piece of legislation, but there is no question that we will vote on this piece of legislation today and we will pass this legislation” (Cong. Rec. S10990). The following day, October 26th, it was enacted into law by the President’s signature. Even today, Congress, through the Cane commission, is still investigating the intelligence failure in preventing 9/11. How could the PATRIOT Act, written within a time frame of less than a month, correctly address the issues that could have prevented 9/11?

Within a short period of time, the PATRIOT Act was written, debated, signed, sealed, and delivered. Expediency, however, has cost Americans much more than just tax money and protection. Some of America’s most fundamental civil liberties were signed away on October 26th of 2001. Congress, yet to learn its lesson, passes the PATRIOT Act, reverting America’s security situation to a time when the government willingly practiced vastly overreaching powers in the name of foreign intelligence.

The USA PATRIOT Act

Indeed many changes in the PATRIOT Act are not just “modest tinkerings” that most experts described the act to be at its inception in 2001 (Breton, A5). The impact of the “tinkerings” has vast impacts on the civil liberties of immigrants, foreigners, and, most abhorred, the citizens of the United States. When approving the PATRIOT Act on October 26, 2001 President Bush stated, “This government will enforce this law with all the urgency of a nation at war,” giving the impression that we are more like a country in the midst of battle rather than a civil nation (Lawrence 5). The country, with legislation like the PATRIOT Act, has now entered into a panicked state similar to the times of COINTELPRO and McCarthyism. Yet, in each instance, the country has reflected on these events and realized the error of its ways. After crucial evaluation of the provisions provided for the PATRIOT Act, it is clear that similar resentment could occur.

The intention of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001 is exactly what it suggests – the protection of America against
terrorism. Indeed, there are some useful and positive aspects to the PATRIOT Act that will, in all frankness, protect America from terrorism and could prevent another tragedy such as 9/11. Connecting the ties between intelligence agencies has long been needed, and efforts to remove such barriers are a major part of the act. For years, our Department of Justice and Central Intelligence Agencies have suffered from a lack of connection and cooperation to exchange needed information. Borders will be fortified with more manpower and monetary resources, critical towards preventing known or potential terrorists from entering the country illegally or legally. The new focus on money laundering schemes is also an important step towards stopping terrorism by allowing seizure of bank accounts and stopping monetary flows from terrorist organizations to their cells and suppliers. Other provisions try to provide aid and support for those who suffer the most in the fight against terrorism. For example, there is a continued effort to protect innocent Muslim and Arab Americans from being ostracized after September 11th, recognizing that their citizenship, their casualties that day, and the attacks that have occurred because of their cultural and religious affiliations (Sec. 102). Though the declaration may not explicitly provide protection, the PATRIOT Act clearly recognizes the predicament Arab Americans face. Moreover, Title VI: Providing for the Victims of Terrorism, Public Safety Officers, and their Families, provides guidelines not only for victims who have suffered in the events of 9/11 but also for subsequent terrorist victims of future attacks. These sections are necessary and should be put into legislation for the benefit of Americans.

The issue at hand, however, is not whether the Act will provide protection; rather, conflicts arise when discussing what price American people will pay for its protection. As Senator Russ Feingold (D-WI), the only member of Senate to vote nay to the Act in October 2001, stated on the floor,

> Of course, there is no doubt that if we lived in a police state, it would be easier to catch terrorists. If we lived in a country that allowed the police to search your home at any time for any reason; if we lived in a country that allowed the government to open your mail, eavesdrop on your phone conversations, or intercept your email communications; if we lived in a country that allowed the government to hold people in jail indefinitely based on what they write or think or based on mere suspicion that they are up to no good, then the government would no doubt discover and arrest more terrorists (S11020).

Indeed if we lived in a “Big Brother” state or in a world where eyes peered through our television like the world of Ray Bradbury’s *Fahrenheit 451*, America would be safe from terrorism and events like September 11th may have been prevented. The moral dilemma is: what are we protecting if we sacrifice those principle liberties that the nation was founded on? The balance between civil liberties and security must be struck.
Moreover, the PATRIOT Act creates a series of imbalances between the three branches, especially between Congress and the Executive Branch. Although there are certain provisions written to curb such potential abuses, they are weak and are ineffective means of oversight. For example, the “sunset provisions” imply that certain sections of the Act will be inactivated without Congress re-approving those particular provisions again in December 2005. The sunset provisions are only found in Title II and only deal with new surveillance and intelligence collection procedures, not with amendments hindering civil liberties. The rest of the PATRIOT Act, lacking these sunset provisions, is permanent.\(^4\) Moreover, for the “sunset” provisions to actually be effective, it requires that Congress continually check up on the progress of the legislation. Unfortunately, since the passing of the PATRIOT Act, Congress has been unable to oversee the actions of the DOJ and law enforcement effectively. Provisions for Congressional oversight are weak, in general, because of their vague requirements and loopholes allowing the DOJ to evade Congressional requests for pertinent information.

As a whole, the PATRIOT Act alters pre-existing legislation in such a way that it risks fundamental, Constitutional rights. Attorney General John Ashcroft, one of the main proponents of legislation, openly declared at a conference in June of 2003 entitled, “Journalism and Homeland Security,” that the methods proposed by the PATRIOT Act were, indeed, not new but merely laws that were being modified to apply to fighting terrorism. Mr. Ashcroft misses a very important point. Though some provisions are only modifications of pre-existing laws, the changes in wording and the addition of particular adjectives have given the DOJ and the Executive Branch unprecedented power to probe into lives of all Americans. The lack of oversight and review, combined with the broad expanses of power now available to the agencies of the executive branch, have made the PATRIOT Act a very powerful piece of legislation that limits the people’s capacity to curb and prevent abuses like those of the past.

**The USA PATRIOT Act**

**Title I: Enhancing Domestic Security Against Terrorism**

Within Title I, Section 106, entitled *Presidential Authority*, the PATRIOT Act amends the International Emergency Power Act to provide broad powers to the President for confiscating property when the United States is being attacked by “any foreign person, foreign organization, or foreign country that he determines has planned, authorized, aided, or engaged in

\(^4\) As a point of contention, there are “sunset-like” clauses in Title III that declare that there are some provisions that can be inactivated in October of 2005 should Congress deem necessary. The difference between these and those found in Title II is that these Congress has to vote for them to be removed, while the “sunset provisions” have to be voted to be kept in.
such hostilities or attacks against the United States; and all right, title, and interest in any property so confiscated shall vest, when, as, and upon the terms directed by the President.” Further, by declaration of the President, “interest or property shall be held, used, administered, liquidated, sold, or otherwise dealt with in the interest of and for the benefit of the United States” (Sec. 106(1)(B)). Not mentioned, though, is specifically when the President may confiscate such property – a loophole that allows the President to confiscate property while an investigation is pending rather than waiting until the investigation is over. Therefore, the confiscation of land like that practiced during the time of Japanese internment camps can once again be repeated, and the idea of “innocent until proven guilty” is no longer applicable. Moreover, as mentioned previously, once confiscated, there is no restriction as to what the President wishes to do with the land, even if the suspect has not yet been proven guilty. One can thus be cleared of all charges, released, and then realize their house or business has been removed entirely.

**Title II: Enhanced Surveillance Procedure**

Title II is arguably one of the most controversial aspects of the PATRIOT Act. Though it may be extreme to declare that Title II is “COINTELPRO II,” it is justifiable to say that the new expansions proposed are not far from its predecessor. Title II reverses many of the existing policies back to a time that is reminiscent of Hoover’s FBI and McCarthyism. The ability to tap into the personal lives of citizens, all in the name of terrorism, has been greatly expanded within these provisions.

One of the Act’s most sweeping changes has been the amendment instituted to alter the manner in which Foreign Intelligence Surveillance Act (FISA) now operates. As previously covered, FISA was created as a way to check the abuses of power possible in the intelligence community by authorizing special search and seizure operations relating to federal investigations of “agents of a foreign power” operating in the United States. However, with amendments to FISA and the expansion of the possible scenarios in which surveillance activities are now “legal,” the checks and balances in place to limit the expansive powers of the Justice Department and the intelligence agencies have been greatly undermined.

The court is now an ineffective blockade against the abuses of civil liberties. Because the Act expands the scope of approved warrants and expands the number of judges and term length from seven and seven, respectively, to eleven judges (Sec. 208), appointments to the court can become so politicized that hawkish members of government can place “appropriate” judges who will serve as agonists to the intelligence process, instead of unbiased actors who are subject to
removal. Moreover, intrusive investigations can occur for even longer, as the FISA surveillance period has been increased to 120 days, and search and seizure period from 45 to 90 days (Sec. 207 (a)(2)(A)).

The PATRIOT Act, in section 218, amended § 1804 (a)(7)(B) of FISA replacing “the primary purpose” with “a significant purpose.” This particular amendment changed a mere three words, but redefined an entire act. On March 6, 2002 Attorney general Ashcroft issued a memorandum outlining the administration’s interpretation of the amendments to FISA. The new procedures are intended to supersede the three DOJ memos discussed above. The Ashcroft memo interprets the PATRIOT Act to allow “FISA to be used primarily for a law enforcement purpose, as long as a significant foreign intelligence purpose remains” (Ashcroft). The memo states that intelligence officers using FISA are authorized to “consult” with federal law enforcement offices to ‘coordinate efforts to investigate or protect against’ foreign threats to national security” (Ashcroft). The two parties now “may exchange a full range of information and advice concerning such efforts in FI or FCI investigations” (Ashcroft). Ashcroft further contends that the Attorney General:

    can most effectively direct and control… investigations only if all relevant DOJ components are free to offer advice and make recommendations, both strategic and tactical, about the conduct and goals of the investigations.

The memo calls for complete cooperation between the FBI and CRM. The drastically different standards between the 1995 and the 2002 Attorney General guidelines came to a head in a case before FISC.

    The Executive Branch now has free reign to fully involve prosecutors and FBI agents in foreign intelligence and surveillance operations. Ashcroft said that the ruling, in confirming the Department of Justice’s “legal authority to integrate fully the function of law enforcement and intelligence,” was “a victory for liberty, safety, and the security of the American people” (“Surveillance Ruling”). Jameel Jaffer, an attorney for the American Civil Liberties Union, had a predictably different reaction to the decision. He said the decision “essentially renders judicial oversight of FBI surveillance meaningless” (“Surveillance Ruling”). However, only Ashcroft had the final word as the ACLU and others watched from afar.

    One clause that has been producing the most attention is called the “sneak and peak” warrants. Created so that evidence and indictments can be attained expediently, Section 213 of the PATRIOT Act allows investigators to secretly enter (physically or electronically) into the “spaces” (offices, apartments, dorms, lockers, etc.) of suspects, collect evidence that is

5 The word primarily is underlined in the memo. The emphasis is not an addition by the authors of this paper.
not tangible (i.e. copies, transferring files, and pictures are some of the things allowed), and leave without posting any sort of notice (i.e. warrant). Moreover, Subsection (3) of Sec. 213 allows the investigator to withhold “[a warrant] within a reasonable period of its execution, which period may thereafter be extended by the court for good cause shown.” Thus, not only can seizures now occur without notifying the suspect, who can be either a foreign national or a U.S. citizen, the courts reserve the right to delay this notification. Clearly, this violates the rights provided by the 4th Amendment which protect citizens against unreasonable search and seizures, which plainly states the necessity of a warrant supported by oath or affirmation. Furthermore, the purpose of a warrant is to provide the courts with the power to grant permission for investigators to enter the private spaces of suspects, upon probable cause. However, Sec. 213, which does not sunset in 2005 (i.e. is permanent), anybody’s home can be subject to search and seizure as long as there is a “possibility” that he or she is associated with terrorism, all without prior court notification or prior notification of the suspect.

Under Section 215, entitled “Access to Records and Other Items Under the Foreign Intelligence Surveillance Act,” sections 501 through 503 of FISA have been struck through to include new provisions that allow the Director of the FBI, and subsequently FBI staff, the ability to “make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution” (PATRIOT Act Sec. 215). The PATRIOT Act eliminates what FISA previously declared the “agent of foreign power” standard, authorizing the FBI access to particular categories of information. Instead, it creates a catch-all provision allowing the FBI to gather any record it may want (even if that record does not deal with a specific person, i.e. the entire record), and allows investigations to take place as long as they are not conducted “solely” on the basis of activities protected by the Constitution. David Cole, author of *Terrorism and the Constitution* addresses the fear that exists in all who realize the breadth of such legislation:

The implications of this change are enormous. Previously, the FBI could get the credit card records of anyone suspected of being a foreign agent. Under the PATRIOT Act, the FBI can get the entire database of the credit card company. Under prior law, the FBI could get library borrowing records only by complying with state law, and always had to ask for the records of specific patron. Under the PATRIOT Act, the FBI can go into a public library, or who used it on a certain day, or who checked out certain hotel or motel, hospital, or university – merely upon the claim that the information is “sought for” an investigation to protect against international terrorism or clandestine intelligence activities (167).
Arguably, there are sections which provide for congressional oversight that seem to be useful in counterbalancing the new, expansive powers given to the Justice Department. FISA now states that:

the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402 (b). On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period -- (1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and (2) the total number of such orders either granted, modified, or denied (Sec. 502 50 USC 1862).

Absent from the report, though, are the types of search and seizures taking place, the items seized, the ultimate fate of the items seized – information that is imperative towards evaluating whether or not civil liberties are being violated.

**Title IX: Improved Intelligence**

On the reform side, Title IX provides a lot of changes towards information sharing amongst intelligence agencies. Title IX greatly expands the capabilities of information sharing in the name of terrorism. In all honesty, information sharing between the agencies has been pitiful, and regarding the release of the 9/11 commission, there is a strong belief that one of the recommendations of the Cane Commission will be greater integration between the agencies, so that information that is passed between intelligence communities can prevent a tragedies like 9/11. Section 905 authorizes the Attorney General and subsequent law enforcement to “[disclose] of foreign intelligence acquired in criminal investigations [and] notice of criminal investigations of foreign intelligence sources” to the Director of Central Intelligence (Sec. 905). However, as Cole states, “[While] the sharing of information makes sense, Congress essentially removed any checks on the mixing of intelligence and law enforcement functions, failing to address the very real concerns that the foreign intelligence approach may lead to serious invasions of liberty of people residing here” (Cole, 160). Sharing of intelligence should and will be used in the fight against terrorist activities. However, like any powers that are given to any branch of government, there should be checks and balances. The National Security Act (NSA) of 1947 makes it explicitly clear that the purpose of the Central Intelligence Agency is not to deal with domestic affairs. Though there is a very strong argument for the necessity of information sharing, there is an eminent fear that the CIA will begin to interfere with domestic criminal investigations and violate the provisions of the NSA.
The Patriot Act in Action

It has been over two years since the PATRIOT Act came into effect. Though there was an initial fear amongst congressmen over the lack of oversight the day the Act was passed, it is evident today that they overestimated the effectiveness of congressional oversight provisions in preventing the Executive Branch’s overreaching powers. Since its passing, the PATRIOT Act has reached the cover of the national press many times because of the inability of the courts and Congress in addressing issues presented by overreaching executive branch agencies. History once again found a way to repeat itself. The ability of Congress to oversee the changes and actions taken by the current administration and the intelligence organizations continue to frustrate our system of checks and balances.

As early as August of 2002, less than a year since the PATRIOT Act’s passing, there were very prevalent signs that it was not being checked. Adam Clymer of the New York Times reported on August 15, 2002, that the “Justice Department has rebuffed House Judiciary Committee efforts to check up on its use of new antiterrorism powers in the latest confrontation between the Bush Administration and Congress over information sought by the legislative branch” (A21). From the House Judiciary Committee, both Rep. Sensenbrenner (R-WI) and Rep. Conyers (D-MI) sent a list of 50 questions to Attorney General Ashcroft pertaining to the use of the new powers in the act, and have received replies only to “simple” questions that do not reveal intricate information pertinent towards intelligence gathering. Even the Senate Judiciary Committee appears to be encountering blockades from the current administration. Sen. Patrick J. Leahy (D-VT), one of the writers of the PATRIOT Act and one of its strongest supporters as is shown by his remarks on the Senate floor when the Act was passed on October 24th, comments, “Since I’ve been here, I have never known an administration that is more difficult to get information from that the oversight committees are entitled to.” Though formerly praising the amount of oversight available in October 2001, he now has to resort to issuing subpoenas to force replies; and moreover, he feels that the Justice Department has taken a position of “we will tell you what we want you to know, and we won’t tell you anything else” (A21). Furthermore, it seems as though, while Congress used to maintain some sense of Congressional oversight over law enforcement agencies, the passing of the PATRIOT Act has forced that relationship to deteriorate. Prof. Harold H. Koh of the Yale Law School, is reported to have observed that “the PATRIOT Act might be the first example of when ‘traditional’ law enforcement is moved under the umbrella of foreign intelligence surveillance, the more difficult it will be to continue the traditional Congressional process of oversight of law enforcement activities” (A21). The more blurred the line becomes between regular law
enforcement agencies and the U.S. foreign intelligence agencies, the harder it will become to decide when to regulate intelligence gatherings and when not to thus inhibiting the U.S. Government’s ability to oversee the actions of its intelligence agencies.

In the November 23, 2003 issue of the *New York Times*, the front page contained an article that delved into the FBI’s new investigatory power which allows the agency to deal with everything from “suspected” terrorists to anti-war movements. Eric Lichtblau of the New York Times reports, “The Federal Bureau of Investigation has collected extensive information on tactics, training and organization of antiwar demonstrators and has advised local law enforcement officials to report any suspicious activity at protests to its counterterrorism squads,” on the belief that these anti-war groups probably have among them people associated with terrorist groups or that a member is a known terrorist (A1). Though the FBI contends that the intelligence-gathering effort was “aimed at identifying anarchists and ‘extreme elements’ plotting violence, not at monitoring the political speech of law-abiding protestors,” the question arises as to how the government can guarantee the privacy of law-abiding citizens. How does one draw the line between potential terrorism and civil disobedience? Again, though implemented with the greatest intention of preventing terrorism, the room for abuse is great.

Moreover, more and more cases are showing up in criminal court system. On November 18, 2003, two federal appeals court judges on the Second Circuit were reported as being “hostile” to the Bush administration’s stance on the requirements of the anti-terror effort “meant that the President could indefinitely detain an American who was arrested in this country as an ‘enemy combatant’ and deny him contact with his lawyer” (Glaberson, A19). The case involved Jose Padilla, who was believed to be planning an explosion of a radiological “dirty bomb.” Mr. Padilla, an American citizen, was detained, has not been allowed to see a lawyer, has been held *incommunicado*, but has not been formally charged with any crime. On one hand, the government was arguing that the nature of the conflict today implied that military principles, not the usual rules of the American criminal courts, had to be applied to “protect the country properly,” and that the President’s power has always included the power to detain military enemies (Glaberson, A19). On the other hand, the two judges vehemently argued that it was a civilian case, making the detention of Mr. Padilla shocking because of the “ease with which” the government transposes military rules into the civilian sphere (Glaberson, A19). Judge Barrington D. Parker, Jr., opposing the government’s actions, is reported to “[believe] that only Congress could make what he describes as an unprecedented decision that would permit the indefinite detention without charges of an American in this country” (Glaberson, A19).
Over the past two years, it has become more apparent to the people who created the Act, especially those in Congress, that the broad expanse of power given to the agencies of the Executive branch was too much. However, the power not only lies in the unprecedented room to abuse Constitutional rights but also in the lack of possibilities for congressional oversight – creating a very powerful document for the government to abuse the civil liberties of its citizens legally.

**The Turning Tide**

Though the Act does provide for a wide expanse of power, the past few years have also proven that even if the agencies of the executive branch see the implementation of the PATRIOT Act’s provision as their right, it will continue to be fought at all levels. If there is any sign of unrest in the public against the PATRIOT Act, it can be found in the libraries of America, where librarians have been making headlines over the past few months by refusing to obey the PATRIOT Act’s provision of allowing government agencies to gather documents and databases of all borrowing records. Though they may not be facing the government’s most intrusive acts, as it reported that only a handful of documents from libraries have been collected out of the thousand or so classified documents, they have been making the most noise and the most head way in fighting the PATRIOT Act: “The old stereotype of librarians as meek maidens whose only passion is for the ‘Dewey Decimal System’ is now being shattered for good, replaced by a new image of librarians as feisty fighters for freedom” (Lichtblau, “Ashcroft’s”, A14). Over the past few months librarians across the nation have been deleting parts of their database as information is stored, especially borrowing records of their customers. As Eric Lichtblau of the *New York Times* comments, “There is a way in which reading is a stand in, and a reading list a short-hand, for life of the mind, an interior life, that librarians rightly feel ought not to be violated. It’s not so much the reading itself they sense need protecting, but what makes us want to read” (“Ashcroft’s”, A14).

Congress has also been partaking in an about face. Many congressmen, especially after seeing the difficulties in practicing any sort of Congressional oversight under the new provisions, are fighting to reform the PATRIOT Act. “In the two years since the act was passed…some federal lawmakers have become more vocal in expressing unease over the use of the expanded surveillance and detention powers” (Irwin). Moreover, over the past two years, it has become more apparent that many members of Congress have looked back on those October 2001 days with much regret. Representative Don Young (R-AK), though noted as an extreme conservative who voted for the Act in 2001, said in a radio interview that the
passage of the PATRIOT Act was “stupid” (Talbot, F19). Jeff Lungren, a spokesman for Representative F. James Sensenbrenner Jr. (WI), chairman of the House Judiciary Committee, expressed similar sentiments when there was a push by those like Sen. Hatch (R-UT) who wished to speed up the process of approving the sunset provisions, stating that extending the life of the PATRIOT Act “will happen over his dead body” (Lichtblau, “Aftereffects” A1). Democrats rallied and helped reject a motion in May 2003 to extend the laws past 2005; and in July of 2003, Congress continued its campaign to reduce the powers provided in the PATRIOT Act, by voting 309 to 118 in favor of scaling back the “sneak and peak” provisions which allowed authorities to conduct searches and seizures without immediately notifying the target of the investigation (Lichtblau, “Threats and Responses: Civil Liberties” A17).

**Conclusion**

With the wisdom provided by a history mixed with success and failure, it is has become increasingly evident that protections are necessary to safeguard the American public from those in positions of authority who seek to misuse their power. In the U.S. system of checks and balances, one should be ever wary that one branch, given near limitless powers, would pursue policies aimed at advancing their agenda and strengthening their influence at a price normally thought too great to bear. As discussed throughout this paper, the intelligence community and the Executive have far overreached their powers numerous times in the past, often in the struggle to secure the nation against threats of a foreign and subversive nature. In each case, the government has taken a reactive position, continually attempting to correct and modify the Executive’s power and authority to act in relation to proper supervision and oversight, not a more constructive position of attempting to prevent new and future infringements of fundamental rights. If history has taught anything, the government, and Congress specifically, should realize that at times when the perceived threat is the greatest, the potential for abuse is equally great; indeed, it is of immense importance during these times to protect against such abuse, not to issue mandates for the contravention of already precarious liberties. The PATRIOT Act stands as "a wish list of powers long sought by federal law enforcement and investigative agencies, chiefly the FBI…The act now gives them the force of law" (Michaels, 38). Not only does the PATRIOT Act modify FISA and the FBI warrant procedures in a manner which allows investigations to be conducted in a broader and more autonomous fashion, but it also stands as a clear indication that the government and perhaps the public at large have implicitly acquiesced to the possibility that the Executive can invade and disrupt the lives of American citizens, reminiscent of the tactics of COINTELPRO. What is needed, rather than an amplification of the
investigative power of the Executive at the cost of proper oversight and accountability, is more consensus, more intense
oversight which includes not only a reactive judiciary but also a constructive, proactive Congress, and more candidness about
what freedoms are being taken away in order to protect the United States from terror. Only after a nation weighs the costs of
a domestic war on terror can it strike the proper balance between freedom and safety.

Appendix

Church Committee Report

“Too many people have been spied upon by too many Government agencies and too much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone ‘bugs’, surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens. Investigations of groups deemed potentially dangerous—and even of groups suspected of associating with potentially dangerous organizations—have continued for decades, despite the fact that those groups did not engage in unlawful activity. Groups and individuals have been harassed and disrupted because of their political view and their lifestyles. Investigations have been based upon vague standards whose breadth made excessive collection inevitable. Unsavory and vicious tactics have been employed—including anonymous attempts to break up marriages, disrupt meetings, ostracize person from their profession, and provoke target groups into rivalries that might result in death. Intelligence agencies have served the political and personal objectives of presidents and other high officials. While the agencies often committed excesses in response to pressure from high official in the Executive branch and Congress, they also occasionally initiated improper activities and then conceal them from officials whom they had a duty to inform.

Governmental officials—including those whose principal duty is to enforce the law—have violated or ignored the law over long periods of time and have advocated and defended their right to break the law.

The Constitutional system of checks and balances has not adequately controlled intelligence activities. Until recently the Executive branch has neither delineated the scope of permissible activities nor established procedures for supervising intelligence agencies. Congress has failed to exercise sufficient oversight, seldom questiong the use to which its appropriations were being put. Most domestic intelligence issue have not reach the courts, and in those cases when they have reached the courts, the judiciary has been reluctant to grapple with them.”

-Church Committee Report (5-6)
# The Foreign Intelligence Surveillance Court: 2003 Membership

<table>
<thead>
<tr>
<th>Name</th>
<th>Date Appointed</th>
<th>Term Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colleen Kollar-Kotelly (DC)</td>
<td>5/19/02</td>
<td>5/18/09</td>
</tr>
<tr>
<td>Harold A. Baker (IL)</td>
<td>5/18/98</td>
<td>5/18/05</td>
</tr>
<tr>
<td>Robert C. Broomfield (AZ)</td>
<td>10/01/02</td>
<td>5/18/09</td>
</tr>
<tr>
<td>Stanley Brotman (NJ)</td>
<td>7/15/97</td>
<td>5/18/04</td>
</tr>
<tr>
<td>James G. Carr (OH)*</td>
<td>5/19/02</td>
<td>5/18/08</td>
</tr>
<tr>
<td>John E. Conway (NM)*</td>
<td>5/19/02</td>
<td>5/18/07</td>
</tr>
<tr>
<td>Michael J. Davis (MN)</td>
<td>5/18/99</td>
<td>5/18/06</td>
</tr>
<tr>
<td>Nathaniel M. Gorton (MA)</td>
<td>5/18/01</td>
<td>5/18/08</td>
</tr>
<tr>
<td>Claude M. Hilton (VA)</td>
<td>5/18/01</td>
<td>5/18/07</td>
</tr>
<tr>
<td>George P. Kazen (TX)</td>
<td>5/18/03</td>
<td>5/18/10</td>
</tr>
<tr>
<td>James Robertson (DC)*</td>
<td>5/19/02</td>
<td>5/18/06</td>
</tr>
</tbody>
</table>

*These three judges were appointed as part of the four judge expansion created by the Patriot Act amendments to FISA. They will not serve full seven year terms in order to allow for the staggering of the appointments.*
Mr. L. Ralph Mecham  
Director, Administrative Office  
of the United States Courts  
Washington, D.C. 20544

Dear Mr. Mecham:

This report is submitted pursuant to the Foreign Intelligence Surveillance Act of 1978, Title 50, United States Code, Section 1807, as amended.

During calendar year 2002, 1228 applications were made to the Foreign Intelligence Surveillance Court for electronic surveillance and physical search. The Court initially approved 1226 applications in 2002. Two applications were "approved as modified," and the United States appealed these applications to the Foreign Intelligence Surveillance Court of Review, as applications having been denied in part. On November 18, 2002, the Court of Review issued a judgment that "ordered and adjudged that the motions for review be granted, the challenged portions of the orders on review be reversed, the Foreign Intelligence Surveillance Court's Rule 11 be vacated, and the cases be remanded with instructions to grant the United States' applications as submitted..." Accordingly, all 1228 applications presented to the Foreign Intelligence Surveillance Court in 2002 were approved.

Sincerely,

John Ashcroft
**Literature Review**

Ashcroft, John. “Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations conducted by the FBI.” 6 March 2002. 30 Nov. 2003


Irwin, Jim. “ACLU Leader highlights questions about Patriot Act.” San Francisco Gate. 8 Nov. 2003, late. ed: ?.


--- “Congressional Supervision of America’s Secret Agencies: The Experience and Legacy of the Church Committee.”

Lawrence, J. M. “WAR ON TERRORISM; Anti-terror laws in place; Feds urgently implement crackdown.”


Reno, Janet. “Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations.” 19 July 1995. 30 Nov. 2003


<www.fas.org/irp/agency/doj/fisa/dag080601>


