# NOTE

# THE IMPACT OF A KNEE-JERK REACTION: THE PATRIOT ACT AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT AND THE ABILITY OF ONE WORD TO ERASE ESTABLISHED CONSTITUTIONAL REQUIREMENTS

## I. INTRODUCTION

The attacks of September 11th sparked a new era in American political and legal history, altering the disposition of the nation's citizens and the legal community from a feeling of comfort and tranquility to vulnerability and paranoia. A result of this vulnerability was the knee-jerk reaction by the government to erect protective barriers to fortify the nation from external threats, and consequently permit surveillance techniques not previously validated by the judiciary, which threatened the individual privacy rights of American citizens. One legal response to the attacks was the amending of the Foreign Intelligence Surveillance Act ("FISA") by the U.S.A. Patriot Act to require "the *significant* purpose," rather than "the purpose," of warrantless surveillance to be foreign intelligence gathering.[1] This change in language had the stated purpose of deconstructing a Department of Justice ("DOJ") policy, created and imposed by the Department due to the misinterpretation of FISA by both the DOJ and the FISA court, which prevented communications between foreign intelligence agents engaged in FISA authorized surveillance and criminal prosecutors.[2] By amending the language of FISA to remedy an inter-departmental policy, the Patriot Act authorized surveillances of American citizens below the previously established constitutional limits.

This Note argues that the history of warrantless surveillance and

---

1. 50 U.S.C. § 1804(a)(7)(B) (Supp. 2005) (emphasis added); *see infra* Part III for a discussion of the motivating factors behind the change in language in addition to the treatment of this language by the FISA court system.

2. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 79 (Official Gov't Edition), *available at* http://www.9-11commission.gov/report/911Report.pdf [hereinafter THE 9/11 COMMISSION REPORT] (stating that the procedures imposed by the DOJ upon communications between foreign intelligence agents involved in FISA surveillance and criminal prosecutors "were almost immediately misunderstood and misapplied" and resulted in "far less information sharing and coordination between the FBI and the Criminal Division in practice than was allowed under the department's procedures"); *see infra* Part IV for further discussion of the DOJ's interpretation and application of FISA procedures and requirements.

judicial interpretation of FISA did not require the restriction of communications, referred to as the "wall," between foreign intelligence and law enforcement agents and that in its current form, the Patriot Act exceeds the judicially established constitutional limitations for warrantless wiretapping of foreign agents for national defense purposes, authorizes unreasonable and illegal searches of American citizens, and remedies a DOJ problem which did not require legislative action.

Part II of this Note examines the history of warrantless electronic surveillance. Part III analyzes FISA as the government's attempt to clarify the standard for permissible warrantless electronic surveillance. Part IV addresses the judicial response to FISA, the confusion of courts over whether to apply the "primary purpose" or "purpose" test, and the DOJ's misinterpretation of the FISA, leading to the imposition of the communications barrier. Part V examines the post-September 11th response of the government and how the Patriot Act made it easier for the administration to combat terrorist threats while rejecting accepted constitutional standards of surveillance and significantly infringing the privacy interests of Americans. Part V also argues that the significant purpose language of FISA, as amended by the Patriot Act, was not necessary to remove the barrier on communications between agents within the DOJ engaged in FISA surveillance and further, that the amended language permits the executive branch to conduct unconstitutional surveillances without acquiring a warrant as mandated by the Fourth Amendment. Part VI proposes multiple legislative amendments to FISA and a DOJ regulation which would cure the unconstitutional practices authorized by the Patriot Act. Part VI also identifies the most recent abuses of FISA as supporting the need for reform and analyzes the inadequacies of Congress's and the Administration's current proposals to amend FISA. Part VII concludes that although the executive branch has the inherent duty and power to protect the nation from threats of violence, the Patriot Act grants the executive unchecked and ill-defined powers to conduct surveillance on American citizens. The Patriot Act, while noble in purpose, requires amending, as the policies and procedures it authorizes with respect to FISA impair the rights of Americans to be free from unreasonable searches and provides the executive with the authority to perform unconstitutional surveillance of American citizens.

## II. HISTORY OF WARRANTLESS ELECTRONIC SURVEILLANCE AND THE ORIGINS OF THE WALL

Warrantless electronic surveillance by the government for foreign

and domestic purposes has had a tumultuous history, varying in acceptance depending upon who was sitting on the Supreme Court, occupying the White House, or serving as the Attorney General.[3] In 1928, the Supreme Court in *Olmstead v. United States*, approving the use of warrantless wiretaps by the Bureau of Prohibition, then the branch of the Department of the Treasury entrusted with enforcing and investigating violations of the National Prohibition Act, held that wiretapping in general does not violate the Fourth Amendment where a physical search or seizure of tangible property or effects did not occur.[4] Wiretapping by the Bureau of Prohibition continued uninhibited through the early 1930s until Congress intervened in 1934 by passing the Federal Communications Act ("FCA"), making it illegal for "any person 'to intercept and divulge or publish the contents of wire and radio communications.'"[5] Three years later, the Supreme Court in *Nardone v. United States* interpreted the FCA to forbid wiretapping by the federal government and deemed information acquired through such methods inadmissible in court.[6] However, the President and the DOJ misinterpreted *Nardone* as permitting warrantless wiretapping for national security purposes and prohibiting the use of information acquired through such wiretaps outside the federal justice system.[7] In a letter from President Roosevelt to his Attorney General, Robert Jackson, the President asserted his view that electronic surveillance would be proper under the Constitution where "grave matters involving the defense of the nation" were involved.[8] The President, limiting his endorsement of the practice, insisted that warrantless electronic investigations be "conducted to a minimum and to limit them insofar as possible to aliens."[9] Unresolved, however, were whether the President's

3. *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 310 n.10 (1972).

4. 277 U.S. 438, 466 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967). Prior to this decision, Attorney General Stone, considering the use of warrantless wiretaps unconstitutional, tyrannical, and brutal, forbade the FBI to use such methods as tools in their criminal law enforcement activities. S. REP. NO. 94-755, at 23 (1976). The *Olmstead* decision marked the first phase in judicial interpretation of the Fourth Amendment, whereby the court considered the act of wiretapping, conducted without a physical search or seizure of tangible property or effects, to be lawful. *Olmstead*, 277 U.S. at 466.

5. S. REP. NO. 95-604, at 10 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3911 (quoting The Federal Communications Act of 1934, 47 U.S.C. § 605 (1964), *invalidated by* TWC Cable Partners v. Cableworks, Inc., 966 F. Supp. 305 (D.N.J. 1997)).

6. 302 U.S. 379, 382, 384 (1937).

7. S. REP. NO. 95-604, at 10.

8. Letter from Franklin D. Roosevelt, President of the United States, to Robert H. Jackson, Att'y Gen. (May 21, 1940) *reprinted in* ROBERT J. LAMPHERE & TOM SHACHTMAN, THE FBI-KGB WAR: A SPECIAL AGENT'S STORY 102 (1986).

9. Letter from Franklin D. Roosevelt, President of the United States, to Robert H. Jackson, Att'y Gen. (May 21, 1940) *reprinted in* ROBERT H. JACKSON, THAT MAN: AN INSIDER'S PORTRAIT

order was limited to domestic subversion and which activities posed a threat to the national defense.[10]

From 1940 to 1965, the director of the FBI continued to authorize warrantless wiretaps to monitor foreign intelligence matters and domestic criminal activities for national security purposes, regardless of the existence of a physical trespass.[11] In March 1965, Attorney General Nicholas Katzenbach amended the DOJ's policy for warrantless wiretapping by requiring prior approval by the Attorney General and limiting an individual wiretap to a period of six months.[12] President Johnson further restricted wiretapping by prohibiting warrantless wiretapping by all federal agencies, except in matters involving national security investigations—which he failed to clearly define—and then only with prior approval by the Attorney General.[13] These new policies were the standard used by the DOJ for warrantless electronic surveillance until 1967 when the Supreme Court again entered the debate and overruled its decision in *Olmstead.*

In the 1967 *Katz v. United States* decision, the Supreme Court abandoned its tresspassory analysis of the Fourth Amendment from *Olmstead* and instead inquired into the expectation of privacy of the target of the electronic surveillance to determine the legality of the surveillance.[14] The Court held that a microphone installed on the side of a public telephone booth without a warrant violated the Fourth Amendment.[15] In so holding, the Court concluded that where a person has a reasonable expectation of privacy, be it in his or her home, apartment, or a closed telephone booth, and that expectation is one that society is prepared to recognize, physical or electronic trespass and surveillance will implicate the Fourth Amendment and require a warrant.[16] Since the Fourth Amendment protects people and not merely places from unreasonable searches and seizures, the Court held that the reach of the Amendment "cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[17] While extending the breadth of the Fourth Amendment in matters of domestic criminal

---

OF FRANKLIN D. ROOSEVELT 68 (2003).

10. S. REP. NO. 94-755(II), at 27-28 (1976); *see also* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 310 n.10 (1972) (asserting that "it is questionable whether this language was meant to apply to solely domestic subversion").

11. S. REP. NO. 95-604, at 11-12.

12. S. REP. NO. 94-755(III), at 285-86 (1976).

13. S. REP. NO. 95-604, at 12.

14. 389 U.S. 347, 351-52, 354 (1967).

15. *Id.* at 352.

16. *Id.* at 352-53.

17. *Id.* at 353.

surveillance, the Court expressly declined to comment on whether additional safeguards, other than prior approval by a neutral magistrate, would satisfy the Fourth Amendment in matters involving national security.[18] While *Katz* gave the Fourth Amendment more teeth regarding the ability to restrict electronic surveillance by the government, the Court left unanswered the question of the legality of warrantless wiretapping for national security and foreign intelligence purposes.

Due in part to the *Katz* decision and the growing uncertainty of the constitutional limits of warrantless electronic surveillance, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[19] Title III prohibited all electronic surveillances except those conducted by law enforcement officers engaged in criminal investigations of certain serious crimes where the officer is able to demonstrate probable cause.[20] However, the law did not restrict

> the power of the President to obtain information by such means as he may deem necessary to protect the Nation from attack or hostile acts of a foreign power, to obtain intelligence information essential to the Nation's security, and to protect the internal security of the United States from those who advocate its overthrow by force or other unlawful means.[21]

Title III, however, did not excuse the President from the requirement of securing a warrant for all national security related electronic surveillances. Instead, as declared in an accompanying report by the

---

18. *Id.* at 358 n.23. Unclear from the Court's decision, however, is if they intended to define national security to encompass foreign intelligence surveillance. Regardless, the Court did not express an opinion as to the constitutionality of warrantless wiretapping when the target was an agent of a foreign power or posed a threat to national security and the issue remained unresolved.

19. S. REP. NO. 95-604, at 12 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3911-14; Omnibus Crime Control and Safe Streets Act of 1968, P.L. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000)).

20. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2511(1), 2517(5), 2518(1)(d) (2000); *see also* United States v. Arnold, 773 F.2d 823, 829 (7th Cir. 1985) (declaring that the "framers of Title III presumably intended by this requirement [judicial approval of the wiretap] to prevent evasion of the several restrictions upon original applications (e.g., showing of probable cause, enumerated serious crime, ineffectiveness of other investigatory techniques as to that offense)").

21. S. REP. NO. 90-1097, at 66 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153. Codified in 18 U.S.C. § 2511(3) (1970) (repealed 1978), the law stated that:

> Nothing contained in this chapter . . . 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.

*Id.* Unresolved from this language was what is considered a threat to national security and who is to determine which acts pose such a threat.

Senate Committee on the Judiciary, the law defined the national security exception to the warrant requirement as applicable only in situations involving a threat to the safety of the nation from foreign powers.[22] In a section entitled "National Security," the Committee concluded:

> It is obvious that whatever means are necessary should and must be taken to protect the national security interest. Wiretapping and electronic surveillance techniques are proper means for the acquisition of counterintelligence against the hostile action of foreign powers. Nothing in the proposed legislation seeks to disturb the power of the President to act in this area. Limitations that may be deemed proper in the field of domestic affairs of a nation become artificial when international relations and internal security are at stake.[23]

While not expressly limiting or defining the national security exception, the manner in which the Committee fashioned its discussion indicated that a warrant would not be required where electronic surveillance is conducted on foreign threats to the safety of the nation. By not establishing the warrant requirement for electronic surveillances for foreign intelligence purposes, and failing to define those actions which threaten national security, Title III lead to further speculation regarding the constitutionality of such warrantless surveillance.

Although warrantless surveillance for foreign intelligence and national security purposes had been conducted since the 1940s, the Supreme Court expressly avoided the issue until 1972.[24] In the 1970 *United States v. Smith* opinion, the Central District Court for California concluded that in entirely domestic scenarios, a warrant is required under the Fourth Amendment even where the situation involves national security.[25] The *Smith* court, in the all too familiar narrowly tailored fashion of the Supreme Court, limited its holding to domestic surveillance, declaring that "it might very well be that warrantless surveillance of this type [national security purposes], while unconstitutional in the domestic situation, would be constitutional in the area of foreign affairs."[26] The Fifth Circuit Court of Appeals in *United States v. Clay* also failed to address what legal requirements were necessary to conduct warrantless wiretapping for foreign intelligence purposes.[27] These opinions failed to clarify the national security

22. S. REP. NO. 90-1097, at 69.

23. *Id.*

24. United States v. Smith, 321 F. Supp. 424, 426 (C.D. Cal. 1971).

25. *Id.* at 429.

26. *Id.* at 426. The court recognized this possible divergence in constitutionality due to the long recognized inherent power of the executive to conduct foreign relations. *Id.*

27. United States v. Clay, 430 F.2d 165, 171 (5th Cir. 1970), *rev'd*, 403 U.S. 698 (1971). The

exception regarding foreign threats to the safety of the nation, in addition to failing to define those activities which pose a threat to national security.

Since Congress had not addressed the executive's ability to conduct warrantless electronic surveillance for national security purposes, the Supreme Court intervened to establish the appropriate constitutional standard in the 1972 decision of *United States v. United States District Court for the Eastern District of Michigan* ("*Keith*").[28] In *Keith*, the Supreme Court addressed the constitutional limits of the President's power, acting through the authorization of the Attorney General, to conduct warrantless electronic surveillance in matters of national security which targeted defendants with no known ties to a foreign power.[29] In this case, the government engaged in warrantless electronic surveillance for the stated purpose of protecting the nation from domestic threats to national security, the prevention of the destruction of government property, and because they overheard one of the defendants plotting to destroy government property.[30] In determining the constitutionality of the executive's surveillance methods, the Court held that because the Fourth Amendment is not absolute in its terms, courts must balance "the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression," to determine the reasonableness and legality of the search.[31] The Court ultimately concluded that the protection of the Fourth Amendment extends to domestic security surveillances conducted without prior judicial approval.[32] A warrant and prior approval by a neutral and detached magistrate were thus required for the government to install electronic surveillance devices to intercept

---

Court in *Clay*, while applying the balancing test from *United States v. U.S. Dist. Court (Keith)*, 407 U.S. 297 (1972), avoided an in-depth analysis of the legality of warrantless foreign intelligence surveillance since the information obtained by the government was not used to prosecute the defendant. *Id.*

28. *Keith*, 407 U.S. 297 (1972).
29. *Id.* at 299.
30. *Id.* at 300-01.
31. *Id.* at 314-15.
32. *Id.* at 316-17, 321. The Court further expounded that:

> Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the executive branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute.

*Id.* at 316-17. The Court's recognition that executive officials cannot be neutral and detached was proved accurate by the abuse of the FISA system by such officials through misrepresentations of fact in applying for FISA surveillance orders. *See infra* Part VI.D for a discussion of these recent abuses.

conversations of persons with no ties to a foreign power.[33]

While the Court recognized the requirement for a warrant in this particular case, it also noted that the Fourth Amendment is not static; rather, the government may bypass the warrant requirement where the government interest outweighs the intrusiveness of the search.[34] In situations involving domestic national security surveillance, the Court concluded that the target of such surveillance "may be less precise than that directed against more conventional types of crime," as the nature of such surveillance differs from ordinary crime in that it involves the interrelation of various sources, types of information, and targets.[35] Although the Court expressed no opinion as to the Fourth Amendment's requirements for electronic surveillance conducted for foreign intelligence purposes, in holding that the standards for national security surveillances may diverge from the standards for ordinary criminal surveillances, the Court implied that foreign intelligence surveillances, where the foreign target poses a threat to national security, may not require a warrant. Consequently, the Court left the executive branch with the unchecked power to conduct warrantless surveillance in situations where the executive perceives a threat to national security from a foreign power or its agents.[36]

In addition to not defining foreign intelligence or addressing the President's ability to conduct warrantless electronic surveillance for foreign intelligence purposes, the Court in *Keith* failed to establish how subsequent courts were to distinguish between typical criminal activities and national security threats. The Court recognized that the President has the duty to "preserve, protect and defend the Constitution of the United

33. *Keith*, 407 U.S. at 318. The Court recognized that although requiring judicial approval of surveillance for domestic national security purposes will impose "some added burden . . . upon the Attorney General, this inconvenience is justified in a free society to protect constitutional values." *Id.* at 321. This quotation by the Supreme Court identifies the ongoing issue of to what degree may the individual liberties guaranteed by the Constitution be sacrificed or trampled on for the sake of national security.

34. *See id.* at 322-23.

35. *Id.* at 322. Though the Court failed to specify how the sources, information, and targets of a national security surveillance differ from ordinary law enforcement, the Court further supported its decision to excuse domestic national security surveillances from the warrant requirement by declaring that these surveillances prevent "unlawful activity" and enhance "the Government's preparedness for some possible future crisis or emergency." *Id.* Thus, due to the pending threat to national security, such surveillances are excused from the strict procedural hurdles of ordinary criminal law.

36. However, in failing to address the legal requirements for warrantless surveillance of a foreign power, the Court also failed to define what constitutes a threat to national security and what degree of connection to a foreign power an individual or group must have to escape the warrant requirement.

States,"[37] implicitly empowering him to "protect our Government against those who would subvert or overthrow it by unlawful means."[38] Under this authority, the President may lawfully "employ electronic surveillance to obtain intelligence information on the plans of those who plot unlawful acts against the Government."[39] However, the Court also pointed to the legislative history of Title III to recognize that Congress, in addition to the courts, were uncertain which activities pose a threat to national security.[40] On the floor of the Senate, Senator Hart stated:

> [W]e are agreed that this language should not be regarded as intending to grant any authority, including authority to put a bug on, that the President does not have now.
>
> In addition, Mr. President, *as I think our exchange makes clear, nothing in section 2511(3) even attempts to define the limits of the President's national security power under present law, which I have always found extremely vague . . . . Section 2511(3) merely says that if the President has such a power, then its exercise is in no way affected by title III*.[41]

This statement recognized that though the President has the inherent power to act in the interest of national security, what was included in that power was uncertain as of 1972. By not identifying those criminal activities which pose a threat to national security, the Court failed to define the scope of the President's inherent national security power and establish a means for courts in the future to determine if the President exceeded this power. This oversight by the Court essentially gave the executive the ability to escape the Fourth Amendment requirements and conduct surveillance without a warrant of activities by American citizens where the executive defines the criminal act as a threat to the national security with a minimal connection to a foreign power.[42]

After *Keith*, three Circuit Courts of Appeal ruled that the Fourth Amendment does not require the executive to secure a warrant when conducting foreign intelligence surveillance that targets a foreign

---

37. *Keith*, 407 U.S. at 310 (quoting U.S. CONST. art. II, § 1).
38. *Id.*
39. *Id.*
40. *Id.* at 306.
41. *Id.* at 307 (emphasis added).
42. As will be examined in Part VI.D, even after Congress enacted FISA, the executive branch abused its ability to conduct warrantless surveillances by submitting over one hundred applications to the FISA court with factual misrepresentations regarding the degree to which the targets of surveillance are connected to a foreign power. Such abuse again highlights the need to curtail the executive's power in this area in order to ensure that FISA is not used as a means to escape the warrant requirement of the Fourth Amendment.

power.[43] Though these courts permitted foreign intelligence surveillance without a warrant, still unanswered were the questions of what degree of the surveillance must be directed towards foreign intelligence and whether there could be an accompanying criminal prosecutorial purpose to the foreign intelligence surveillance. The Fourth Circuit of the United States Court of Appeals answered these questions and established the constitutional requirements for warrantless electronic surveillance for foreign intelligence purposes in *United States v. Truong Dinh Hung*.[44] The defendant in *Truong* was convicted by the district court of espionage for delivering classified government documents to representatives from the Socialist Republic of Vietnam.[45] The issue on appeal was the constitutionality of the government's warrantless wiretapping of the defendant's phone under the claim of a foreign intelligence exception to the Fourth Amendment.[46] The court affirmed the inherent constitutional authority of the executive branch to conduct foreign intelligence surveillances, though the scope of this power was not defined by the court, and declared that a warrant is not required each time the executive conducts such surveillance as it would inhibit the executive's ability to counter national security threats.[47] However, recognizing that individual privacy interests may be infringed upon were the executive allowed to conduct foreign intelligence surveillance with no prior judicial authorization, the court limited the executive's ability to conduct such surveillance without a warrant to situations where the target of the surveillance is a foreign power or its agent and "the surveillance is conducted 'primarily' for foreign intelligence reasons."[48]

In applying the primary purpose language, the *Truong* court admitted evidence which had been obtained prior to July 20, 1977, but excluded evidence obtained through the warrantless wiretaps after that

43. United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977) (stating that foreign security wiretaps are a recognized exception to the warrant requirement); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (en banc) (holding that prior judicial authorization was not required where surveillance was conducted and maintained solely for the purpose of gathering foreign intelligence information. The court further held that the strong public interest in protecting from attacks on the government permits courts to rely on the good faith assertion by the executive that the surveillance is for foreign intelligence purposes); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) (holding warrantless wiretapping by the executive to be lawful due to the President's inherent power to safeguard the nation from "possible foreign encroachment").

44. 629 F.2d 908 (4th Cir. 1980).

45. *Id.* at 911-12.

46. *Id.* The government, in an effort to discover the source of the classified diplomatic cables and papers Truong was attempting to pass to representatives from the Socialist Republic of Vietnam, tapped Truong's telephone for 255 days without seeking prior court authorization. *Id.* at 912.

47. *Id.* at 913, 914.

48. *Id.* at 915.

date.[49] The court accepted the district court's conclusion that between July 19th and 20th, the surveillance of Truong became primarily focused on criminal investigation, established by memoranda circulated between the DOJ and other national security agencies.[50] "Although the Criminal Division of the Justice Department had been aware of the investigation from its inception," this did not invalidate the surveillance since its primary focus was foreign intelligence gathering until July 20th.[51] In its analysis, the court recognized that all foreign intelligence surveillances are in part criminal investigations and rejected the government's contention that "if surveillance is to any degree directed at gathering foreign intelligence, the executive may ignore the warrant requirement of the Fourth Amendment."[52] The court also limited the Administration's warrantless foreign intelligence surveillance powers by declaring that "once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination."[53] Using the balancing test from *Keith*, the court concluded that an exception to the Fourth Amendment warrant requirement does exist, but only when the primary purpose of the surveillance is to gather information regarding foreign powers, their agents, and their collaborators.[54] The primary purpose test was thus the constitutionally required standard where the executive branch conducted warrantless surveillance of a foreign power or their agents or collaborators within the United States.[55]

While requiring that the primary purpose of the executive's surveillance be foreign intelligence, the court did not prohibit communications between criminal investigators and foreign intelligence agents while warrantless foreign intelligence surveillances were ongoing. As the court previously recognized, all foreign intelligence surveillances are in part criminal investigations and communication

---

49. *Id.* at 916.

50. *Id.*; *see also* United States v. Humphrey, 456 F. Supp. 51, 59 (E.D. Va. 1978) (describing the July 19th memoranda as stating for the first time "that probable cause existed to charge both defendants," and the "July 20 letter from the Attorney General to the Director of Central Intelligence" as proof of that "the Justice Department [is] trying to put together a criminal case. A similar letter to Zbigniew Brzezinski, Assistant to the President for National Security Affairs . . . contains this sentence: 'The State Department and the CIA have been requested to make the necessary documents and witnesses available for use at trial.'").

51. *Truong Dinh Hung*, 629 F.2d at 916.

52. *Id.* at 915.

53. *Id.* The court noted that such court review of the executive's surveillance is necessary since "individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution." *Id.*

54. *Id.* at 916.

55. *Id.* at 915.

between the two divisions is expected and permissible, so long as the focus of the surveillance does not become primarily criminal investigation.[56] Clearly, the court did not intend to prohibit communication between divisions of the DOJ.

During the course of the trial and subsequent appeal of the *Truong* case, Congress enacted FISA to establish the procedural requirements for the executive to conduct warrantless wiretapping of a foreign agent.[57] The *Truong* court, while recognizing "that the imposition of a warrant requirement, beyond the constitutional minimum described in this opinion, should be left to the intricate balancing performed in the course of the legislative process by Congress and the President,"[58] still maintained that the executive may only be excused from the warrant requirement "when the surveillance is conducted 'primarily' for foreign intelligence reasons" and the subject of the search or surveillance is a foreign power.[59] The court justified its position by stating that "it would be unwise for the judiciary, inexpert in foreign intelligence" to establish the procedural requirements governing foreign intelligence surveillance where the legislature and the executive are more familiar with the nature and structure of foreign intelligence surveillance.[60] While the court clearly declared that the primary purpose standard was the standard upon which warrantless intelligence surveillance involving a foreign agent must be conducted, it refused to impose procedural barriers or limit the government's ability to impose a warrant requirement beyond the minimum established in the opinion.[61] The court's establishment of the primary purpose standard for excusing the executive from obtaining a warrant for foreign intelligence surveillance, as will be examined later, was accepted by a majority of courts examining the constitutionality of FISA surveillance.

## III. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

Congress passed the Foreign Intelligence Surveillance Act, or FISA, in 1978 to provide a procedure through which the Attorney General could conduct warrantless electronic surveillance for foreign intelligence purposes within the United States with prior judicial authorization, though not requiring the criminal standard of probable

56. *Id.* at 916.
57. *Id.* at 914 n.4.
58. *Id.*
59. *Id.* at 915.
60. *Id.* at 914 n.4.
61. *Id.*

cause.[62] The law was designed to limit the collection and use of information regarding United States citizens and legal aliens "acquired from electronic surveillances to matters properly related to foreign intelligence and the enforcement of criminal law."[63] The law effectively repealed the inherent power of the executive to engage in electronic surveillance for foreign intelligence purposes and instead required prior judicial approval before engaging in such surveillance. Both the text of FISA and the legislative history indicate that Congress anticipated that the information collected pursuant to a FISA surveillance order would involve evidence of criminal activities, which would be used in the prosecution of criminals. A wall prohibiting communication between the foreign intelligence division and the criminal division of the DOJ while acquiring foreign intelligence specified in the FISA order, as will be discussed, was neither articulated nor anticipated by FISA.

FISA established a strict set of guidelines which the applying executive agency must follow prior to securing an order to conduct electronic surveillance upon a foreign power or their agents.[64] The law

---

62. S. REP. NO. 95-604, at 5 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3906-07; *see also* United States v. Mayfield, 504 F. Supp. 2d 1023, 1032 (D. Or. 2007) (declaring that instead of the Fourth Amendment probable cause standards, FISA requires that there exists "'probable cause' to believe that the target of the search or surveillance is a foreign power or an agent of a foreign power").

63. S. REP.NO. 95-604, at 6.

64. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (2000) (defining a foreign power as

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

The law defined an "[a]gent of a foreign power" as

> (1) any person other than a United States person, who— (A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a) (4) of this section; (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or (2) any person who— (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; (C)

permitted federal officers to apply to the Foreign Intelligence Surveillance Court ("FISA court") for a FISA order requesting authorization to conduct surveillance on a foreign agent, but only after the Attorney General certified that the surveillance will target a foreign power or its agent and that the targeted facility is being used or is about to be used by a foreign power or its agent.[65] Upon submission of the application to the FISA court for approval, the Assistant to the President for National Security Affairs or an executive branch official as designated by the President, must certify that the purpose of the surveillance is to obtain foreign intelligence information and that the information cannot be obtained through the use of normal investigative techniques.[66] The law defined foreign intelligence information as:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—(A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States.[67]

The law further required the Attorney General to adopt certain minimization procedures to limit the "acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons" used as evidence of a crime or other law enforcement purposes.[68]

Although FISA defined "[f]oreign intelligence information" with relative clarity, within that definition, the "national defense or the security of the United States" was not defined with certain specificity.[69]

---

> knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; or (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).).

*Id.*

65. *Id.* § 1804(a).
66. *Id.* § 1804(a)(7)(A)-(D).
67. *Id.* § 1801(e).
68. *Id.* § 1801(h)(1).
69. *Id.* § 1801(e)(2)(A); *see also* Exec. Order No. 12,958, 60 Fed. Reg. 76 (Apr. 17, 1995)

The failure of Congress to articulate which activities fall under this national security classification allows surveillance of a foreign power or an agent of a foreign power where the executive deems the target of surveillance as a threat to national security. Further lowering the burden on the executive to secure a FISA order, the law allowed a FISA court judge to approve of the requested surveillance where the judge determines that the evidence presented by the executive official is "not clearly erroneous."[70] In so concluding, the judge is not required to conduct an in-depth probe into the validity of the information presented in the application, and instead makes his determination based on the executive official's certification.[71] Due to the great deference given to the executive branch to certify that the target of surveillance is a national security threat with a connection to a foreign power and the minimal inquiry required by the FISA judge into the validity of the facts, FISA fails to effectively safeguard from abuse possible targets of surveillance by the executive and authorizes surveillance of United States persons engaged in alleged criminal activities which have garnered Fourth Amendment protection in the past.

The text of FISA clearly anticipated that foreign intelligence information collected pursuant to a FISA order would be used for criminal prosecution purposes. Congress defined the targets of FISA surveillance—a foreign power or its agent—as any person who "knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the Unites States."[72] In addition to the targets of surveillance, FISA defined the activities which may be monitored as those which involve a "violation of the criminal laws of the United States or of any State, or that would be a criminal violation if

---

(defining national security as "the national defense or foreign relations of the United States"). Although numerous courts have applied the definition of national defense as asserted in this executive order, this definition fails to identify those particular criminal activities which pose a threat to the nation.

70. 50 U.S.C. § 1805(a)(5).

71. *See* S. REP. NO. 95-701, at 10 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3978 (declaring that "[i]n such cases [of foreign intelligence] the judge is fully informed of (but does not review) the basis for the certification and is given a detailed description of the nature of the information sought and a statement of the means of surveillance to be used"). Due to the minimal inquiry required of the judge into the validity of the facts presented, even though the law does require judicial approval, it is not a sufficient safeguard to ensure that the facts are accurate and that the information sought is primarily for foreign intelligence surveillance purposes. *See infra* Part VI.B for a discussion of the failure of the FISA court to identify hundreds of factual misrepresentations in the applications for FISA orders by the executive branch.

72. 50 U.S.C. § 1801(b)(2)(A).

committed within the jurisdiction of the United States or any State."[73] By defining the targets of FISA surveillances to include those individuals and acts which violate United States criminal laws, the law clearly anticipated that criminal prosecution would result from such surveillances and that in procuring such information, criminal investigators could communicate and coordinate with the foreign intelligence agents responsible for conducting the FISA search.[74]

Section 104(a)(7)(B) of FISA is most frequently cited as establishing the unsubstantiated wall preventing communication between foreign intelligence agents and criminal investigators.[75] This section requires that the certifying executive official attest to the fact that the FISA order for surveillance is being sought for "the purpose of . . . obtain[ing] foreign intelligence information."[76] While the text of FISA failed to explain Congress's intended definition of the word "purpose," it clearly allowed for the use of FISA acquired information in criminal proceedings "with the advance authorization of the Attorney General."[77] The Senate Intelligence Committee, however, made clear in its accompanying report that the primary purpose of the surveillance must be for foreign intelligence.[78] The Committee recognized that:

> [T]he standards and procedures for electronic surveillance differ according to whether the primary purpose is collecting foreign intelligence [to enable the government to understand and assess the capabilities, intentions, and activities of a foreign power] or assisting foreign counterintelligence and counterterrorism investigations [to protect against clandestine intelligence activities, sabotage, and terrorism by or on behalf of foreign powers].[79]

While the Committee recognized that the procedural requirements for electronic surveillance may vary based on the nature of the surveillance, the primary purpose of FISA surveillance must remain foreign

---

73. *Id.* § 1801(c)(1).

74. The interpretation of FISA permitting communication between the criminal and foreign intelligence divisions within the DOJ, in addition to being based on the law's anticipation that criminal prosecutions would result from such surveillance and that those acts which were the focus of surveillance violated the criminal statutes of the United States, is furthered by the failure of the text of FISA to expressly restrict or mention any limitation on such communications.

75. *See infra* Part IV for a discussion of the origins and affirmation of the restriction on communications within the DOJ.

76. 50 U.S.C. § 1804(a)(7)(B).

77. *Id.* at § 1806(b) (stating that "[n]o information acquired pursuant to this title shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General").

78. S. REP. NO. 95-701, at 9 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3978.

79. *Id.*

intelligence gathering.

FISA and the accompanying committee reports, despite the requirement that FISA authorized surveillances must have the primary purpose of foreign intelligence gathering, anticipated that information collected through FISA surveillances would be used in criminal prosecutions and that the foreign intelligence agents engaged in FISA surveillance could coordinate with federal law enforcement officers. In addition to defining the information that may be acquired through a FISA order to include intelligence activities which "'involve or will involve a violation' of the criminal law,"[80] the House and Senate Committees expressly permitted and anticipated that information acquired through FISA surveillance may be used for the enforcement of criminal law.[81] The Senate Committee on the Judiciary, further supporting the contention that Congress did not intend to erect a wall preventing communication between criminal prosecutors and foreign intelligence agents, interpreted the minimization procedures as requiring that FISA acquired information "not be *used* for an unrelated purpose (other than for enforcement of the criminal law)."[82] The Committee further stated that in a criminal matter, the minimization procedures ensure that the tapes and files documenting the foreign intelligence information "will be retained in their original state so that when criminal prosecutions are undertaken it is clear that evidence is intact and has not been tampered with."[83] Although the Committee admitted that information obtained through FISA surveillance may be used in criminal proceedings, the Committee expected these cases to be few in number since the primary purpose of FISA surveillance is not to gather evidence of criminal activity, but rather to obtain information regarding foreign intelligence activities as defined under FISA.[84] Based on the anticipation by both the Senate and House Committees that information collected

---

80. S. REP. NO. 95-604, at 16 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3917 (internal quotation omitted); *see also* S. REP. NO. 95-701, at 21; H.R. CONF. REP. NO. 95-1720, at 22 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4051.

81. S. REP. NO. 95-701, at 10-11.

> U.S. persons may be authorized targets, and the surveillance is part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnapping, and terrorist acts committed by or on behalf of foreign powers. Intelligence and criminal law enforcement tend to merge in this area.

*Id.*

82. S. REP. NO. 95-604, at 39; *see also* H.R. CONF. REP. NO. 95-1720, at 22 (concluding that FISA defines the minimization procedures as allowing for the prevention of criminal acts and the enforcement of criminal law).

83. S. REP. NO. 95-604, at 39.

84. *Id.*

pursuant to a FISA order would be used as evidence in criminal prosecutions, the Committees implied that a degree of communication between foreign intelligence surveillance agents and criminal prosecutors must occur, otherwise criminal prosecutors would be unable to access, interpret, and utilize the information collected by the foreign intelligence agents.

Addressing Fourth Amendment concerns regarding FISA surveillance, the Senate Select Committee on Intelligence undertook a balancing test, as conducted in the *Keith* case, where the government's interest in national security is weighed against the intrusiveness of the surveillance to the targeted individual.[85] The Committee concluded that the additional procedural safeguards imposed by FISA upon the executive branch allow the less stringent standards implemented by FISA to be constitutional under the standards set forth in the *Keith* decision.[86] The Committee further stated that although FISA surveillance diverges from the traditional Fourth Amendment warrant requirements, it was reasonable and therefore constitutional as FISA created new safeguards for personal privacy while allowing surveillance "in circumstances where, because of uncertainty about the legal requirements, the Government may otherwise be reluctant to use this technique for detecting dangerous foreign intelligence and terrorist activities by foreign powers in this country."[87] Both the text and the history of FISA, while clear that the purpose of a FISA order must be foreign intelligence gathering, precluded neither the use of foreign surveillance information in criminal proceedings, nor the communication between criminal prosecutors and foreign intelligence agents conducting FISA surveillance, as long as the primary purpose of the surveillance remained foreign intelligence gathering.

## IV. JUDICIAL RESPONSE AND THE ORIGINS OF THE WALL

After its enactment, courts reviewing the constitutionality of FISA surveillances disagreed on the interpretation of the language of FISA and the application of the primary purpose standard established by the *Truong* court. Although a majority of courts have concluded that the proper constitutional standard for conducting surveillance pursuant to a FISA order is that the primary purpose be for foreign intelligence

85. S. REP. NO. 95-701, at 12-16.

86. *Id.* at 16. Such procedural safeguards include certification by an executive official of the facts in a FISA order application, approval by the Attorney General of the surveillance, judicial approval of the FISA order by a FISA court judge, and continuous reporting to congressional committees. *Id.* at 10.

87. *Id* at 16.

gathering, a number of courts have refuted this understanding, creating further confusion in the law's application. If this disagreement among courts proves anything, it is that the constitutional standard for warrantless surveillance for foreign intelligence purposes was neither clear nor well established.

Those courts affirming the holding of the *Truong* court, that the primary purpose of warrantless surveillance must be foreign intelligence gathering and extending its application to FISA authorized surveillance, have not excluded information collected pursuant to a FISA order in criminal prosecutions where, at the time the information was collected, it could be reasonably anticipated that a criminal investigation would result.[88] In *United States v. Duggan*, the Second Circuit Court of Appeals held that the requirement that foreign intelligence surveillance "be the primary objective of the surveillance is plain not only from the language of § 1802(b) but also from the requirements in § 1804 as to what the application must contain."[89] The court concluded that the application process, in requiring certification of the presented facts by an executive branch official, ensures that the information sought will be for the purpose of gathering foreign intelligence information.[90] FISA requires that the FISA court "not . . . second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information," effectively requiring the FISA court to presume the executive branch has the purpose of foreign intelligence gathering in applying for a FISA application.[91] However, recognizing that such a presumption may lead to future abuse of FISA surveillance, the court clarified that such a presumption does not "give the government carte blanche to obtain a surveillance order in violation of a target's right to due process" and may be overcome by a substantial showing that "'a false statement knowingly and intentionally, or with reckless disregard for the truth was included' in the application and that the allegedly false statement was 'necessary' to the FISA Judge's approval of the application."[92]

---

88. *See, e.g.*, United States v. Cavanagh, 807 F.2d 787, 790-91 (9th Cir. 1987); United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984); United States v. Belfield, 692 F.2d 141, 146 (D.C. Cir. 1982).

89. *Duggan*, 743 F.2d at 77.

90. *Id.*

91. *Id.* Although the court stated that the FISA application process and executive certification will ensure that the primary purpose of a FISA order will be foreign intelligence surveillance, the court clearly was mistaken based on the hundreds of factual inaccuracies included in FISA order applications submitted by the executive. *See infra* note 121 and accompanying text.

92. *Id.* at 77 n.6 (citation omitted). However, as recognized by the court, the defendant contesting the constitutionality of FISA surveillance does not have a right to review the FISA

In addition to giving deference to the executive in declaring that the primary purpose of the surveillance was for foreign intelligence gathering, the *Duggan* court held that a FISA order is not invalid simply because the executive could anticipate that the fruits of the surveillance would be later used in a criminal trial.[93] The court emphasized that in passing FISA, Congress anticipated that the concerns of the government with respect to foreign intelligence will overlap those with respect to law enforcement.[94] The court ultimately concluded that the mere presence of a domestic law enforcement purpose will not invalidate FISA surveillance where the primary purpose of the surveillance was to gather foreign intelligence information, as certified to by an executive branch official, where the defendant was engaged in international terrorist acts or the plotting of those acts.[95]

While *Duggan* and numerous other circuit court decisions have agreed that the proper constitutional requirement for acquiring a FISA order is that the surveillance be conducted for the primary purpose of gathering foreign intelligence information, numerous courts have simply applied the plain language of FISA.[96] In assessing the validity of a FISA search, these courts have required a showing that the purpose of the surveillance, rather than the primary purpose, was to obtain foreign intelligence information and that such information could not have been acquired through normal investigative techniques.[97] Coincidentally,

---

application and order. Instead, the Attorney General may file an affidavit declaring "that disclosure of the FISA applications and orders would harm the national security of the United States. The judge has the discretion to disclose portions of the documents" which he deems "'necessary to make an accurate determination of the legality of the surveillance.'" *Id.* at 78 (citation omitted). Known as the State Secrets Doctrine, discussed *infra* Part VI.B, the government may invoke this privilege to prevent disclosure to a defendant of what they deem to be documents vital to national security. Though the court hearing a criminal case involving a target of FISA surveillance may review the documents *in camera* and *ex parte* to verify the validity of the executive's claim, such review does guarantee the defendant a fair trial, as he is unable to review all the evidence against him.

93. *Id.* at 78.

94. *Id.*; *see also* S. REP. NO. 95-701, at 11 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3979 (declaring that "[i]ntelligence and criminal law enforcement tend to merge in this area [foreign counterintelligence investigations]").

95. *Duggan*, 743 F.2d at 78; *see also* United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Falvey, 540 F. Supp. 1306, 1313-14 (E.D.N.Y. 1982) (all stating that information acquired through a FISA order may subsequently be used in criminal prosecution where the primary purpose of the surveillance was foreign intelligence gathering and not criminal prosecution).

96. The plain language being "that the purpose of the surveillance is to obtain foreign intelligence information." Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1804(a)(7)(B) (2000).

97. *See, e.g.*, United States v. Cavanagh, 807 F.2d 787, 790 (9th Cir. 1987); United States v. Ott, 827 F.2d 473, 475 (9th Cir. 1987).

these courts held, in accordance with those courts applying the primary purpose test, that where evidence of criminal activity was discovered through a FISA order, such evidence is admissible in a criminal prosecution of the target of the surveillance.[98]

However, the court in *United States v. Belfield*, while applying the statutory language of FISA, asserted that the inquiry required under FISA to determine the legality of the surveillance is easier to satisfy than the pre-FISA requirement.[99] The court noted that before FISA, "courts had to determine whether the surveillance fell within the President's inherent power to conduct electronic surveillance for foreign intelligence purposes."[100] After FISA, courts merely had "to determine whether the application and order comply with the statutory requirements."[101] Through this statement, the *Belfield* court recognized that FISA essentially codified a new standard for assessing the validity of warrantless foreign intelligence surveillance, whereby the court no longer must inquire into the nature of the surveillance by the executive, but, assuming that FISA is constitutional, must determine if the requirements of the statute have been followed. By making this assertion, the court left unresolved the question of whether the purpose standard used in FISA was the equivalent of the primary purpose standard iterated in *Truong*.

In contrast to these courts, the court in *United States v. Sarkissian* explicitly refused to decide if the primary purpose or the purpose test was the requisite standard for a court to apply in reviewing a FISA order.[102] The *Sarkissian* court acknowledged that FISA authorized surveillance need not cease upon the discovery of evidence of a crime and the fact that "the government may later choose to prosecute is irrelevant" to the legality of FISA or the particular surveillance.[103] The court, like other courts applying the primary purpose and the purpose test, held that information obtained through a proper FISA order may be used in a criminal proceeding.[104] Thus, while refusing to conclusively adopt the purpose or primary purpose language, the court allowed the

---

98. *See Cavanagh*, 807 F.2d at 791; United States v. Belfield, 692 F.2d 141, 146 (D.C. Cir. 1982).

99. 669 F.2d at 149.

100. *Id.*

101. *Id.*

102. United States v. Sarkissian, 841 F.2d 959, 964 (9th Cir. 1988) (holding that "[r]egardless of whether the test is one of purpose or primary purpose, our review of the government's FISA materials convinces us that it is met in this case"); *see also In re* Kevork, 634 F. Supp. 1002, 1015 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986).

103. *Sarkissian*, 841 F.2d at 965.

104. *Id.*

use of evidence collected through FISA surveillance in a criminal prosecution, as had previous courts which affirmatively adopted the primary purpose standard. Although courts have failed to reach a uniform conclusion regarding the application of the primary purpose or the purpose language, they have unanimously acknowledged that the gathered information may be used in criminal prosecutions. Despite this uniform agreement by courts regarding the use of FISA acquired evidence for criminal prosecutions, the uncertainty created over which purpose standard the court would apply led to a dramatic change in the manner in which the DOJ coordinated FISA surveillances and criminal investigations.

In response to the majority judicial determination that the primary purpose of FISA surveillance must be for foreign intelligence gathering, in 1995 the DOJ imposed procedures intended to ensure that intelligence gathering, rather than criminal prosecution, remains the primary purpose of foreign intelligence investigations.[105] These procedures, established in a memo by then-Attorney General Janet Reno, declared that "[t]he Criminal Division shall not . . . instruct the FBI on the operation, continuation, or expansion of FISA electronic surveillance."[106] The procedures further required that advice from the FBI to the Criminal Division shall not "result in either the fact or the appearance of the Criminal Division's directing or controlling the FI [foreign intelligence] or FCI [foreign counter intelligence] investigation toward law enforcement objectives."[107] One such imposed procedure was the requirement that the FBI notify the Criminal Division if "facts or circumstances are developed that reasonably indicate that a significant federal crime has been, is being, or may be committed."[108] Although communication between the FBI and the Criminal Division was permissible through the text of FISA and Congressional interpretation of the law, as analyzed and explained *supra* in Part III, the procedures were "almost immediately misunderstood and misapplied" to forbid such communications.[109]

---

105. U.S. DEP'T OF JUSTICE, ATT'Y GEN. REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NAT'L LABORATORY INVESTIGATION 721 (2000), *available at* http://www.usdoj.gov/ag/readingroom/bellows20.pdf [hereinafter THE HANDLING OF THE LOS ALAMOS].

106. Memorandum from Janet Reno, Att'y Gen., to Assistant Att'y Gen., Criminal Div.; Dir., FBI; Counsel for Intelligence Policy; U.S. Att'ys (July 19, 1996), *reprinted in The USA Patriot Act in Practice: Shedding Light on the FISA Process: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 185 (2002).

107. *Id.*

108. *Id.* at 184.

109. THE 9/11 COMMISSION REPORT, *supra* note 2, at 79. In reporting on the attacks of 9/11

Within the DOJ, the language of the procedures was narrowly interpreted to require the Office of Intelligence Policy and Review ("OIPR") to prevent any communication between the FBI and the Criminal Division regarding FISA surveillance.[110] Essentially, the OIPR acted as a wall or gatekeeper between the FBI and the Criminal Division of the DOJ, preventing any communication in order to preserve the admissibility of FISA surveillance information.[111] The procedures were further misinterpreted as preventing the sharing of any foreign intelligence information between those FBI agents working on criminal investigations and those FBI agents conducting foreign intelligence surveillance, even where a FISA order was not used for surveillance.[112] The wall created by the DOJ restricting the flow of information, though it stemmed from the legitimate fear of rejection of a FISA application and the exclusion of FISA surveillance information in a criminal prosecution, had no express statutory or judicial origins. Further invalidating this DOJ policy, no FISA court through 1995 had rejected an application for a FISA order and no court which engaged in a criminal prosecution had suppressed evidence on the basis that the primary purpose of the FISA surveillance was not for foreign intelligence.[113]

In a report filed by the Attorney General's Report Team ("AGRT") analyzing FISA and the DOJ's application of the statute, it states that nowhere in the language of FISA "is there a requirement that the purpose of the underlying *investigation* be inquired into," and in fact, Congress anticipated that the investigation might have a "criminal as well as foreign counterintelligence objective."[114] Since FISA was silent

---

and the events leading up to those attacks, the 9/11 Commission recounted an investigation of a suspect in the bombing of the U.S.S. Cole. In this investigation, an FBI agent, designated as a criminal agent, felt that the procedures required by the FISA court and the DOJ mandated that she could not pursue a lead on the suspect as the information sought was foreign intelligence information of which only intelligence agents could pursue. In a response to an e-mail from the FBI agent, another FBI agent stated: "Whatever has happened to this—someday someone will die—and wall or not—the public will not understand why we were not more effective [in deterring future terrorist attacks] and throwing every resource we had at certain 'problems.'" *Id.* at 271. This statement not only demonstrates the confusion that agents had regarding the required procedures for conducting foreign intelligence surveillance, but it also demonstrates that perhaps the attacks on 9/11 could have been avoided had the courts articulated a clearer standard regarding the required procedures for conducting warrantless electronic surveillance on a foreign agent.

110. *In re* Sealed Case, 310 F.3d 717, 728 (FISA Ct. Rev. 2002).

111. THE 9/11 COMMISSION REPORT, *supra* note 2, at 79.

112. *Id.*

113. *See* U.S. GEN. ACCOUNTING OFFICE, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED 3 (2001).

114. THE HANDLING OF THE LOS ALAMOS, *supra* note 105, at 737.

regarding the requisite purpose of the investigation, the statute only required the surveillance or the search have an intended foreign intelligence purpose,[115] the *Truong* court's interpretation, being the most recent court decision on foreign intelligence surveillance as of 1995, was therefore the judicially mandated constitutional standard for FISA surveillances. As a result of the AGRT report, both the DOJ and Congress were alerted to the significant danger posed by the strict and unfounded communication barrier imposed by the DOJ.[116]

Although the DOJ was correct in its concern for the possible misuse of a FISA order for criminal investigation purposes, their procedural initiatives were more extreme than constitutionally required. A previously classified 1995 memo from Deputy Attorney General Jamie Gorelick to U.S. Attorney Mary Jo White, FBI Director Louis Freeh, Richard Scruggs of the Council of Intelligence Policy and Review, and Assistant Attorney General for the Criminal Division Jo Ann Harris, recognized the need to "prevent any risk of creating an unwarranted appearance that FISA is being used to avoid procedural safeguards which would apply in a criminal investigation" and asserted the necessity of the new procedures restricting communications between criminal and counterintelligence investigators.[117] However, Gorelick also recognized that the procedures "go beyond what is legally required."[118] Even under the primary purpose test, where there was continuing foreign intelligence surveillance, criminal prosecutors could coordinate their efforts with the agents conducting FISA surveillance if the criminal investigation did not dominate or control the surveillance and if the primary purpose of the FISA order was for foreign intelligence surveillance at the time the application was filed and when the Criminal Division became involved.[119] The self-imposed limitations on the communication and coordination between criminal and counterintelligence divisions of the DOJ, in addition to not being legally required, would significantly impair the DOJ's ability to monitor and combat foreign threats and ultimately contribute to the government's inability to prevent the tragic events of September 11, 2001.[120]

---

115. *Id.*

116. *In re* Sealed Case, 310 F.3d 717, 728 (FISA Ct. Rev. 2002).

117. Memorandum from Jamie Gorelick, Deputy Att'y Gen., to Mary Jo White, U.S. Att'y, Louis Freeh, FBI Dir., Richard Scruggs, Council of Intelligence Policy & Rev. & Jo Ann Harris, Assistant Att'y Gen., Criminal Division (1995), *reprinted in* JOHN ASHCROFT, NEVER AGAIN: SECURING AMERICA AND RESTORING JUSTICE 236-38 (2006).

118. *Id.* at 238.

119. *See supra* Part II for the *Truong* court's analysis of the primary purpose standard and acceptable degrees of communication.

120. THE 9/11 COMMISSION REPORT, *supra* note 2, at 271; *see also* Memorandum from Mary

In addition to the limitations on communications, the FISA court imposed further restrictions on the DOJ in 2000 and 2001 upon learning of nearly one hundred errors and omissions in FISA applications presented to the FISA court for authorization of surveillance.[121] The majority of errors in the FISA applications involved misrepresentations about criminal investigations of targets of FISA surveillance and the description of the conducted communications between intelligence agents and criminal prosecutors.[122] As a result, the FISA court required anyone who reviewed "FISA-obtained intelligence . . . to sign a certification acknowledging that the Court's approval was required for dissemination to criminal investigators."[123] Although the FISA court's additional barriers may have contributed to the proliferation of the wall, it was again the misconduct of the DOJ, through misrepresentations and disregard for required procedures, which led to the ineffectiveness of counterterrorism measures.

## V. A SHIFT IN FOCUS: THE USA PATRIOT ACT

On the morning of September 12, 2001, President Bush, commenting to his top advisors about the attacks on the World Trade Center and the Pentagon the previous day, said "[d]on't ever let this happen again."[124] In response, Attorney General John Ashcroft demanded the DOJ change its operational focus: "Prosecution cannot be our priority. If we lose the ability to prosecute, that's fine; but we have to prevent the next attack. Prevention has to be our top priority."[125] This

---

Jo White, U.S. Att'y, to Jamie Gorelick, Deputy Att'y Gen. (1995), *reprinted in* JOHN ASHCROFT, NEVER AGAIN: SECURING AMERICA AND RESTORING JUSTICE 239 (2006).

> [Counterintelligence] is not an area where it is safe or prudent to build unnecessary walls . . . or to compartmentalize our knowledge of any possible players, plans or activities. . . . The single biggest mistake we can make in attempting to combat terrorism is to insulate the criminal side of the house from the intelligence side of the house, unless such insulation is absolutely necessary. Excessive conservatism . . . can have deadly results.

*Id.*

121. U.S. DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS (NOVEMBER 2004) 36 (2006) [hereinafter A REVIEW OF THE FBI].

122. *Id*. at 37 (citing as an example of a DOJ misrepresentation an instance where the FBI submitted an application for a FISA order asserting that the Field Office in New York "had separate teams of agents handling the criminal and intelligence investigations," when in fact "different agents were assigned to the criminal and intelligence investigations, [but] they were not kept separate from each other").

123. *Id*.

124. JOHN ASHCROFT, NEVER AGAIN: SECURING AMERICA AND RESTORING JUSTICE 130 (2006).

125. *Id.* at 133.

shift in focus from prosecution to prevention required access to legal tools previously unavailable to the DOJ while conducting counterterrorism investigations.[126] Less than a week after September 11th, Attorney General Ashcroft and his team of DOJ attorneys drafted legislation providing access to these legal tools in order to more effectively combat terrorism.[127]

On October 26, 2001, after less than two months since the attacks of September 11th and little if any debate in committee or on the floor of Congress, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("Patriot Act") was signed into law by President Bush.[128] Section 218 of the Act amended 50 U.S.C. § 1804(a)(7)(B) of FISA to require the significant purpose of a FISA order be for foreign intelligence, rather than the previously required primary purpose or purpose requirement.[129] By amending the requisite purpose of a FISA order, Congress intended "that the purpose to gather intelligence could be less than the main or dominant purpose, but nonetheless important and not de minimis."[130] The purpose of a FISA order, under the new language, does not have to be primarily for foreign intelligence, rather "gathering criminal evidence could be the primary purpose as long as gathering foreign intelligence was a significant purpose in the investigation."[131] This change in language, while minimizing the degree of factual proof the government is required to demonstrate to obtain a FISA order, contradicted the previously constitutionally required primary purpose standard and threatened the right of Americans to be secure in their communications where they had a reasonable expectation of privacy.

In addition to allowing the government to conduct warrantless searches where the primary purpose was for criminal investigation, the Patriot Act also authorized the sharing of information between criminal investigators and those engaged in foreign intelligence gathering.[132] The act amended 50 U.S.C. § 1806 of FISA by explicitly permitting those

126. *Id.* at 156. As will be discussed, such legal tools included amending the legal standard for acquiring a FISA order and the degree of permissible communications between criminal prosecutors and foreign intelligence agents.

127. *Id.* at 154.

128. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

129. 50 U.S.C. § 1804(a)(7)(B) (Supp. 2005).

130. 148 CONG. REC. S9109, S9110 (daily ed. Sept. 24, 2002) (joint statement of Senators Hatch, Thurmond, Kyl, DeWine, Sessions, & McConnell).

131. *Id.*

132. *Id.*

federal officers engaged in foreign intelligence surveillance under a FISA order to "consult with Federal law enforcement officers . . . to coordinate efforts to investigate or protect against" attacks or other grave hostile acts, sabotage or international terrorism, or clandestine intelligence activities, by foreign powers or their agents.[133] Although FISA never prohibited communications between criminal investigators and those engaged in foreign intelligence gathering, the Administration and Congress saw the Patriot Act as necessary to tear down the wall constructed by the DOJ to prevent such communications and coordination.[134] However, as will be analyzed, the Patriot Act amendments were not necessary to promote better communication or tear down the wall. The Patriot Act amendments codified a new legal standard previously rejected by the courts and invoked a solution to a problem which was not created by the law, but by the policies of the DOJ. These amendments to FISA were unconstitutional and unnecessary to effectuate the goals of the Administration after September 11th.[135]

In 2002, as a result of the passage of the Patriot Act, Attorney General Ashcroft proposed new guidelines governing the execution of FISA approved surveillance, allowing "FISA to be used primarily for a law enforcement purpose, as long as a significant foreign intelligence purpose remains."[136] As a result of the new language, the DOJ sought to remove the self-imposed wall by allowing "intelligence and law enforcement officers . . . [to] exchange a full range of information and advice" regarding foreign intelligence and foreign counterintelligence investigations while FISA surveillance is conducted.[137] Upon submitting the proposed procedures to the FISA court for approval, the court rejected the procedures as inconsistent with the text of FISA *In re All Matters Submitted to Foreign Intelligence Surveillance Court* ("*In re All*

133. 50 U.S.C. § 1806(k)(1) (Supp. 2005).

134. ASHCROFT, *supra* note 124, at 155.

135. *See* Mayfield v. United States, 504 F. Supp. 2d 1023, 1036-43 (D. Or. 2007) (declaring that the significant purpose language of the Patriot Act impermissibly and unconstitutionally allows the government to conduct warrantless surveillance on a United States person. In addition to this language, the court concluded that the degree of deference given to the executive in certifying that the FISA order is accurate, with little judicial inspection as to the validity of this assertion, disregarded the constitutionally required checks and balances of the three branches of government. The court ultimately concluded that 50 U.S.C. §§ 1804, 1823, as amended by the Patriot Act, are unconstitutional.).

136. Memorandum from John Ashcroft, Att'y Gen., to the Dir., FBI; Assistant Att'y Gen., Criminal Div.; Counsel for Intelligence Policy; U.S. Att'ys (March 6, 2002), *reprinted in The USA Patriot Act in Practice: Shedding Light on the FISA Process: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. 180 (2002).

137. *Id.*

*Matters*").[138]

The court in *In re All Matters* concluded that the proposed procedures which authorized criminal prosecutors to communicate with and advise foreign intelligence agents on the "initiation, operation, continuation, or expansion of FISA's intrusive seizures . . . enhance[d] the acquisition, retention and dissemination of evidence for law enforcement purposes, instead of being consistent with the need of the United States to 'obtain, produce, and disseminate foreign intelligence information' as mandated in § 1801(h) and § 1821(4)."[139] By permitting this increased communication, the court held that the "procedures appear to be designed to amend the law and substitute the FISA for Title III electronic surveillances."[140] Since the Patriot Act amendments to FISA did not change the definition of the required minimization procedures, the court concluded that the proposed procedures cannot be used to amend the law in ways Congress has not.[141] Ultimately, the court mandated that law enforcement officers "shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances" or direct or control FISA surveillances to enhance criminal prosecution.[142] However, in condemning the proposed procedures, the court acknowledged that FISA did permit extensive coordination and information sharing with criminal prosecutors, so long as criminal prosecutors do not direct or control the FISA surveillance.[143] Excluded from the court's analysis, however, was a consideration of the impact of the Patriot Act's amendment to FISA allowing for the significant purpose of surveillance to be foreign intelligence. Disagreeing with the outcome of the FISA court, the government appealed the decision regarding the proposed procedures and the amendments to the Patriot Act.[144]

---

138. 218 F. Supp. 2d 611, 624-25 (FISA Ct. 2002).

139. *Id.* at 623 (emphasis omitted).

140. *Id.*; *cf.* Mayfield v. United States, 504 F. Supp. 2d 1023, 1039-41 (D. Or. 2007) (declaring that the USA Patriot Act's amendment to FISA establishing the "significant purpose" test to eliminate the DOJ established "wall" in communications, ignored the fact that even under the "primary purpose" test of FISA, criminal investigators were "free to seek orders authorizing surveillance under Title III, and traditional search warrants that satisfy the Fourth Amendment requirements." The court concluded that Title III, by authorizing surveillance for predicate offenses, "for which surveillance is justified for virtually all terrorism and espionage-related offenses," provides a "satisfactory alternative when criminal investigators cannot have access to FISA surveillance.").

141. *In re All Matters*, 218 F. Supp. 2d at 623.

142. *Id.* at 625.

143. *Id.* at 623-24.

144. *In re* Sealed Case, 310 F.3d 717, 719 (FISA Ct. Rev. 2002).

In its first ever decision, the Foreign Intelligence Surveillance Court of Review ("FISCR") rejected the lower court's findings in *In re All Matters* and affirmed the legality of the Attorney General's proposed procedures and the USA Patriot Act amendments in *In re Sealed Case*.[145] Though the lower court did not address the issue of the constitutionality of the significant purpose test, the government brought the issue before the FISCR, in addition to challenging the lower court's decision concerning the wall. Regarding the wall, the court ruled that the language of FISA never required the restrictions imposed on communications between criminal prosecutors and intelligence officials.[146] The wall, according to the court, instead originated by the FISA court and the DOJ's improper interpretation of FISA.[147] Because FISA defines an agent of a foreign power by requiring a showing of criminal activity, the court found it "quite puzzling that the Justice Department, at some point during the 1980s, began to read the statute as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents—even for foreign intelligence crimes."[148] Based on this analysis, the court concluded that FISA permitted the use of intelligence information in criminal prosecutions and that coordination between foreign intelligence agents and criminal prosecutors is permissible and necessary to protect national security.[149] The FISCR went so far as to suggest that by expressly authorizing communications between criminal prosecutors and intelligence officials, Congress implied that either criminal prosecutors or intelligence officials may direct and control the surveillance.[150]

In addition to rejecting the procedures implemented to limit communications within the DOJ, the FISCR rejected the primary purpose standard as not constitutionally required and impeding effective counterterrorism efforts.[151] In validating the Patriot Act's significant purpose test, the court held that as long as the government maintains the

---

145. *Id.* at 719-20, 746.

146. *Id.* at 721.

147. *Id.*

148. *Id.* at 723.

149. *Id.* at 723, 727, 731.

150. *Id.* at 734. However, as is addressed in Part V.C., this conclusion is unconstitutional as it allows the executive to escape the Fourth Amendment warrant requirement where an executive official certifies that the target of FISA surveillance is a foreign power or its agent, and the court, without delving into the facts too deeply, determines that this certification is "not clearly erroneous."

151. *Id.* at 742-43 (declaring that the primary purpose test drew a line between criminal prosecution and foreign intelligence gathering that "was inherently unstable, unrealistic, and confusing," and additionally, rested on the false premise that "once government moves to criminal prosecution, its 'foreign policy concerns' recede").

possibility of using techniques other than criminal prosecution and articulates "a broader objective than criminal prosecution—such as stopping an ongoing conspiracy—and includes other potential non-prosecutorial responses," the significant purpose test is satisfied and the surveillance is valid.[152] Only where FISA surveillance is conducted for the sole purpose of criminal prosecution will the application be denied.[153] In concluding that the primary purpose test was not constitutionally required, the court inquired into whether the Patriot Act appropriately balanced the protection of individual rights versus the necessity of the government to protect against national security threats, as articulated in the *Keith* case. The court found that the primary purpose test, because it failed to articulate how to determine if surveillance became primarily focused on criminal prosecution, created confusion within the DOJ resulting in a lack of communication, which put the security of the nation at risk.[154] The court concluded that by permitting all FISA surveillance, even where there is an attenuated connection to foreign intelligence, the significant purpose language created a clearer standard to determine the validity of the surveillance and more effectively protected national security without significantly intruding upon individual rights.[155] As a result, the court held that the significant purpose standard satisfied the Fourth Amendment balancing test articulated in *Keith* and was constitutional.[156] It is true that "effective counterintelligence . . . requires the wholehearted cooperation of all the government's personnel,"[157] however, the court failed to seriously consider the extent to which the government could now use FISA as a pretext to circumvent the Fourth Amendment warrant requirement.[158]

---

152. *Id.* at 735.

153. *Id.*

154. *Id.* at 743-44. Additionally, the court announced that "a standard which punishes such cooperation could well be thought dangerous to national security." *Id.* at 743. Clearly, any law which creates confusion and impedes the government's ability to stop an eminent threat to the nation is counterproductive and should not be enacted or enforced. However, the court's critique of the primary purpose standard must be viewed in light of the privacy rights of individual Americans and the possible abuses of those rights by the government. The primary purpose standard ensured that the government obeyed the warrant requirements of the Fourth Amendment, thereby providing sufficient protection of the privacy rights of Americans in all but those situations where a foreign power or its agent posed a threat to the safety of the nation. If the primary purpose standard had been properly interpreted from the outset, the court would not have come to this conclusion nor would the significant purpose amendments have been necessary.

155. *Id.* at 746.

156. *Id.*

157. *Id.* at 743.

158. *Compare id.* (recognizing the need for cooperation between government branches to effectively combat terrorism, though not identifying the danger posed by the lack of deliberate checks and balances between the three branches of government authorized by amendments to

After the FISCR handed down its ruling, because the government was the only party involved, the American Civil Liberties Union ("ACLU") filed a petition for certiorari with the Supreme Court requesting review of the following questions: Whether the Patriot Act permits the government to conduct surveillance under FISA "even where the government's primary purpose is law enforcement rather than foreign intelligence," and if the Patriot Act permits the government to conduct FISA surveillance where the primary purpose is law enforcement, does this standard violate the First and Fourth Amendments.[159] The Supreme Court denied the ACLU's petition to intervene and for a writ of certiorari, refusing to review the FISCR's decision.[160] Although the Supreme Court refused to review the decision, such a refusal is not a judgment on the merits of the lower court's decision.[161] While the current judicial consensus is that the Patriot Act permits FISA surveillance where the primary focus is law enforcement and is permissible under the Fourth Amendment, this law could be overturned by the Supreme Court and should be for reasons discussed later.[162] Although the FISCR had jurisdiction to review the case, it is troubling that the constitutionality of a law authorizing a government practice which implicates significant personal liberty invasions of American citizens has been determined by a court which meets in secret, rarely publishes opinions, has no adversarial process, and has never had a case overturned or reviewed by the Supreme Court.

### *A. Issues: The Problems with the State of the Law*

In drafting the Patriot Act, the goal of the DOJ was to "think outside the box, but inside the Constitution" regarding the new

---

FISA), *with* Mayfield v. United States, 504 F. Supp. 2d 1023, 1042 (D. Or. 2007) (declaring that "the constitutionally required interplay between Executive Action, Judicial decision, and Congressional enactment, has been eliminated by the FISA amendments" which fails to "curtail overzealous executive, legislative, or judicial activity regardless of the catalyst for overzealousness").

159. Petition for Leave to Intervene & Petition for Writ of Certiorari at i, In re Sealed Case of the Foreign Intelligence Surveillance Court of Review, 538 U.S. 920 (2003) (No. 02-001), *available at* http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/fisa/aclufisa21803cpet.pdf.

160. ACLU v. United States, 538 U.S. 920 (2003).

161. *See* Davis v. Balkcom, 369 U.S. 811 (1962) (stating that "the denial of a writ of certiorari does not mean this Court approves the decision below"); Brown v. Allen, 344 U.S. 443, 456 (1953) (declaring "[w]e have frequently said that the denial of certiorari 'imports no expression of opinion upon the merits of a case'") (citation omitted).

162. *Contra* Mayfield v. United States, 504 F. Supp. 2d 1023, 1039, 1042-43 (D. Or. 2007) (declaring that the Patriot Act amended FISA to allow the government to avoid traditional Fourth Amendment judicial oversight used to obtain a surveillance order and is thus unconstitutional).

counterterrorism tools authorized by the law.[163] It is hard to declare that the Patriot Act stayed within the Constitution when the legally required standard for warrantless foreign intelligence surveillances had been established by the court in *Truong* and was subsequently abandoned by the new law. While the motivations behind the Patriot Act were legitimate, the means in which the law addressed these concerns were not.

### *B. The Primary Purpose Standard and Foreign Affairs*

The constitutionality of the original version of FISA and the general practice of warrantless electronic surveillance were uncertain even where the primary purpose was to gather foreign intelligence information. Evidence of the practice's and the law's questionable legality was the inability of the executive branch and the Supreme Court to settle on acceptance or rejection of the practice since 1924 and courts' inability to uniformly approve of the primary purpose standard.[164] Although Title III, the governing law on warrantless surveillance before FISA was enacted, excused the executive branch from securing a warrant for national security related surveillances where a foreign power was involved,[165] the restrictions placed on such surveillance by FISA demonstrated that both Congress and the President understood the possibility for abuse of warrantless wiretapping, especially where the reviewing court plays a limited, if any, role in authorizing such surveillance. The procedural requirements imposed upon the government by FISA further suggest that there is not an unrestrained national security or foreign affairs exception to the Fourth Amendment warrant requirement.[166]

By mandating that foreign intelligence surveillance be the primary purpose of the surveillance, FISA created a means for the government to escape a showing of probable cause where they could prove to a closed court that the target of the requested surveillance has a connection with a foreign power, though how direct and supported this connection must be was not specified.[167] Even more troubling is the fact that the FISA court,

---

163. John Ashcroft, Former U.S. Att'y Gen., Address at Hofstra University: Leadership in Challenging Times (Mar. 20, 2007).

164. *See supra* Parts II & IV.

165. S. REP NO. 90-1097, at 66 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153.

166. S. REP. NO. 95-701, at 71 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4040 (declaring that FISA, by asserting that the provided for procedures "shall be the 'exclusive means by which electronic surveillance . . . [may] be . . . conducted' . . . puts to rest the notion that Congress recognizes an inherent Presidential power to conduct such surveillances in the United States").

167. *See* Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801(b)(2)(A) (2000).

in reviewing an application for surveillance, is not permitted to inquire into the purpose of the surveillance, and instead must rely upon and defer to the certification by an executive official that the surveillance is being conducted for foreign intelligence purposes.[168]

Though it has been well-established that the President is endowed with the inherent power to conduct foreign affairs activities, such deference to the executive branch where warrantless surveillance and troubling invasions of the privacy of Americans exist cannot be permissible. Due to the potential for abuse of Americans' Fourth Amendment rights, the FISA court must not be a rubber stamp for the executive branch to conduct warrantless searches of Americans for alleged foreign intelligence purposes where such connections with a foreign power are not required to be demonstrated to or researched by the court. Although the foreign affairs power may only be exerted by the executive branch of the government, because of the overlap of criminal law enforcement and foreign intelligence and the potential to use information acquired through a FISA order in criminal prosecutions, the FISA court must inquire into the purpose of the surveillance it is authorizing to ensure that the assertions of the executive branch are supported by proof of a substantial connection with a foreign power. Such inquiry by the court, though it may delay the court's authorization of FISA orders, would ensure the right of Americans "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[169] While the purpose of a FISA order could not primarily be for criminal prosecution under the original language, the incredible deference given to the executive branch in establishing and certifying the connection of the target of surveillance to a foreign power failed to ensure that the government's purpose was in fact primarily for foreign intelligence purposes and teetered on the brink of illegality.

In addition to the questionable legality of the procedures mandated by FISA, the language of the law itself was unconstitutional if it authorized surveillance below the constitutionally required standards. In *Truong*, as discussed in Part II, the court noted that the purpose of warrantless electronic surveillance of a foreign agent was primarily for

---

This section permits FISA surveillance of "any person who . . . knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power." *Id.* The standard of proof required to determine the extent of "knowingly," however, is not specified and apparently left up to the FISA court to determine.

168. *In re* Sealed Case, 310 F.3d 717, 736 (FISA Ct. Rev. 2002) (declaring that "the government's purpose as set forth in a section 1804(a)(7)(B) certification is to be judged by the national security official's articulation and not by a FISA court inquiry into the origins of an investigation nor an examination of the personnel involved").

169. U.S. CONST. amend. IV.

foreign intelligence gathering.[170] The courts interpreting and applying FISA have applied this primary purpose standard even though the text of FISA required that foreign intelligence be "the purpose" of warrantless surveillance.[171] Textually, FISA did not require the primary purpose standard. However, the Senate Committee on the Judiciary, in their report on FISA, interpreted the law as requiring that the primary purpose of FISA surveillance be for foreign intelligence gathering and not criminal prosecution.[172] Although it is unclear if the purpose test is the equivalent of the primary purpose standard, if FISA did establish the standard for foreign intelligence below the constitutional requirement set in *Truong*, any surveillance conducted under FISA authorization would be an unreasonable search in violation of the Fourth Amendment and therefore unconstitutional.

### *C. The Patriot Act, the Significant Purpose Standard, and National Defense*

FISA rests on the assumption that surveillance of a foreign power or agent within the United States is necessary and acceptable without a warrant where "the national defense or the security of the United States" is at issue.[173] However, no case, memorandum, Presidential order, or law, including FISA and the Patriot Act, define national security with true specificity.[174] While the need to protect national security is an important government interest, by failing to define what exactly national defense entails, Congress and the courts created a loophole for the DOJ to conduct surveillance of ordinary criminal activities where they are certified by an executive official as threatening the safety of the nation and involving a foreign power or its agent.

In applying for a FISA order, the DOJ may persuasively argue that any domestic criminal activity involving a foreign power or agent threatens to undermine the security of the nation. However, the Fourth Amendment requires a warrant for the majority of government invasions

---

170. United States v. Truong Dinh Hung, 629 F.2d 908, 916 (4th Cir. 1980).

171. *See supra* Part IV, for a discussion of courts' application of the primary purpose test.

172. S. REP. NO. 95-701, at 62 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4031.

173. 50 U.S.C. § 1801(e)(2)(A) (2000).

174. The author recognizes that, in the effort to protect the nation, the executive branch must be able to take action where it perceives a threat to the core operations and general safety of the nation and its people. A definition limiting the executive's power to take action to protect the country would be both dangerous and counterproductive. However, for purposes of this Note, the failure of Congress to define what entails a threat to national security gives the executive a blank check to conduct warrantless electronic surveillance. While this may be a necessary evil to protect the country from foreign threats, it also tramples on the established freedoms of Americans guaranteed by centuries of fighting and sacrifice.

into the personal privacy of American persons, especially for those activities not implicating national security.[175] The fatal flaw with FISA is that it fails to distinguish between those criminal activities by a foreign agent which require Fourth Amendment protection and those activities involving a foreign agent which threaten national security, thereby requiring a FISA order. Although a FISA order has been affirmed as a reasonable search under the Fourth Amendment, the failure of Congress to carefully define those activities which threaten the safety of the nation, and the DOJ's ability to avoid a warrant where a tenuous connection with a foreign power exists, provokes questions of the law's constitutionality.

The Patriot Act amendments to FISA, changing the required intent of the surveillance to the "significant purpose" of foreign intelligence, certainly cannot withstand constitutional scrutiny if the constitutionality of the original primary purpose standard was already a question. The Patriot Act allows the government to forgo the warrant requirement where there is a connection with a foreign power, even though the primary motivation behind the surveillance is criminal prosecution.[176] While national security requires the President to have some latitude when dealing with threats from a foreign power, that exception should not permit the DOJ to use FISA as a pretext to circumvent the Fourth Amendment. The significant purpose standard allows the government to conduct warrantless surveillance for the primary purpose of criminal investigation of any person within the United States with a connection, false or otherwise, to a foreign power.[177] The demonstration of a minimal connection with a foreign power is not a sufficient substitute for probable cause that a crime is being committed or that evidence of a crime will be uncovered.[178] Such blatant disregard for the Fourth

175. *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 310, 314-15, 317 (1972). In declaring that upon review of government surveillance, a court must balance the interest of the government to protect domestic security with the invasion into individual privacies, the court established that where no threat to the security of the nation exists, foreign or domestic, a warrant will be required and the Fourth Amendment standards of probable cause must be demonstrated to a neutral magistrate. *Id.*

176. *See* 148 CONG. REC. S9109, S9110 (daily ed. Sept. 24, 2002) (joint statement of Senators Hatch, Thurmond, Kyl, DeWine, Sessions, & McConnell).

177. *Cf. id.*; *see also* Mayfield v. United States, 504 F. Supp. 2d 1023, 1036 (D. Or. 2007) (identifying the fact that FISA authorizes the government to "conduct surveillance to gather evidence for use in a criminal case without a traditional warrant, as long as it presents a non-reviewable assertion that it also has a significant interest in the targeted person for foreign intelligence purposes." By identifying that the government's assertion is non-reviewable, the court, in rather benign terminology, is criticizing the law for giving such unchecked discretion to the executive in deciding whom to conduct surveillance upon.).

178. *See Mayfield*, 504 F. Supp. 2d at 1036-37. The *Mayfield* court recognized that the significant purpose standard of the Patriot Act effectively eliminated the hard-fought legislative

Amendment and the protected liberties and privacy of all Americans is unconstitutional and cannot withstand the required balancing test set forth in *Keith* to determine the reasonableness of the search. Furthermore, the significant purpose standard cannot withstand constitutional scrutiny as it permits warrantless surveillance below the constitutional minimum standards set forth in *Truong.* While Congress unquestionably has the power to overrule judicially created rules of evidence and procedure that are not constitutionally required, where the Supreme Court has established the constitutional minimum for a certain area of the law, laws which do not meet that minimum standard will be invalid.[179]

As noted in the *Truong* decision, the primary purpose standard and those procedures established by that court for warrantless foreign intelligence surveillance were the constitutionally required standards.[180] The *Truong* court noted that although it declared the constitutional minimum for warrantless wiretapping of a foreign agent, the imposition of warrant requirements for foreign intelligence surveillance beyond those required in the decision should be left to the "intricate balancing performed in the course of the legislative process by Congress and the President."[181] Although the *Truong* court recognized that legislation could be enacted to establish standards for warrantless wiretapping with a less burdensome purpose requirement, such a standard must pass the balancing test of the *Keith* case and not unreasonably interfere with the privacy rights of Americans.[182] Since the Patriot Act did not adhere to the constitutional minimum requiring that warrantless surveillance be conducted for the primary purpose of foreign intelligence, and allows impermissible invasions into the privacy of Americans where the government makes an unsubstantiated and unchecked assertion that the

---

compromise reached by FISA, allowing the government to avoid the Fourth Amendment warrant and probable cause requirements only for national security intelligence gathering, by permitting the executive branch to bypass the Fourth Amendment altogether in gathering evidence for a criminal prosecution.

179. *See, e.g.*, Lane v. Brown, 372 U.S. 477 (1963). In *Lane*, a state officer outside the judicial system was given the "power [by an act of the state legislature] to take from an indigent all hope of any appeal" by refusing to order a transcript merely because he thought the appeal would be unsuccessful. *Id.* at 485. The Court found that "[s]uch a procedure . . . does not meet constitutional standards," and overruled the state legislature's act. *Id.* This case supports the proposition that laws which do not meet the minimum constitutional standard established by the Court will be invalid.

180. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 914 n.4 (4th Cir. 1980).

181. *Id.*

182. *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 314-15 (1972) (stating that it is the duty of the court to determine the reasonableness of surveillance by balancing "the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression").

target has a connection to a foreign power, the significant purpose standard must be struck down as an unconstitutional and unreasonable search in violation of the *Keith* balancing test applied by the court in *Truong*.

### *D. The Fall of the Wall*

One of the primary goals of the Patriot Act was to remove the wall restricting communications between criminal prosecutors and foreign intelligence agents conducting FISA surveillance,[183] by amending the language of FISA to allow surveillance where the "significant purpose" was foreign intelligence. As determined by the FISCR, the wall was artificially created by the DOJ and not legally required by the text of FISA or the interpretation of the law by the courts.[184] The text of FISA and the accompanying congressional reports support the fact that Congress intended the intelligence uncovered by FISA surveillances to be used in criminal prosecutions and that communications between the intelligence agents and criminal prosecutors were permissible and expected.[185] What Congress did not permit was for criminal prosecutors to direct or control FISA surveillance.

While the FISCR was correct in its assessment that the prohibition of communications between foreign intelligence agents and criminal prosecutors was not legally required, the court improperly suggested that either criminal prosecutors or intelligence agents could direct and control FISA surveillance.[186] FISA authorized the use of information uncovered through FISA surveillances in criminal prosecutions and required the significant purpose of the surveillance be foreign intelligence gathering.[187] Under the current language of FISA, criminal prosecutors may coordinate with foreign intelligence agents to acquire a FISA order, direct the surveillance for criminal prosecution purposes, and not be required to demonstrate probable cause as required by the Fourth Amendment. The authorized significant purpose standard dismantled the wall restricting communications; however it had the incidental effect of transforming FISA into a means for the DOJ to

---

183. *See* ASHCROFT, *supra* note 124, at 155.

184. *In re* Sealed Case, 310 F.3d 717, 721 (FISA Ct. Rev. 2002).

185. *See supra* Part III.

186. *See In re Sealed Case*, 310 F.3d at 734 (stating that "when Congress explicitly authorizes consultation and coordination between different offices in the government, without even suggesting a limitation on who is to direct and control, it necessarily implies that either could be taking the lead").

187. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1804(a)(7)(B); *see supra* Part III.

conduct criminal investigations under the guise of foreign intelligence surveillance without the confines of the Fourth Amendment. The moment a criminal prosecutor controls FISA authorized surveillance, FISA becomes a pretext for the government to escape the warrant and probable cause requirements of the Fourth Amendment and unlawfully invades the protected privacy rights of Americans.

## VI. REMEDIES: PROPOSALS TO PROTECT LIBERTY WHILE SECURING THE NATION

Due to the problems asserted with the current provisions of FISA, the government must undertake certain steps to ensure the constitutionality of FISA surveillance and protect the privacy interests of American citizens. Numerous options are available through which the government may remedy the current problems with FISA.

### *A. Legislative Amendment to FISA*

The current language for obtaining FISA surveillance requires only a significant purpose of gathering foreign intelligence information.[188] As explained above, not only does this standard allow surveillance below the constitutionally required primary purpose standard, it also permits the government to conduct surveillance where the primary purpose is criminal prosecution. To remedy the constitutional issues with FISA, Congress must enact legislation which, at a minimum, amends the language of FISA to the primary purpose standard. Though this language may still infringe upon a defendant's Fourth Amendment rights, the primary purpose standard has at least been approved by numerous District and Appellate Courts as reasonable in addition to being the constitutional requirement for foreign intelligence surveillances conducted without a warrant.[189] However, to ensure that FISA is unquestionably constitutional and an appropriate exercise of the President's foreign affairs power, the language of FISA should be amended to require that surveillance be enacted for the "sole purpose of foreign intelligence gathering." Where FISA surveillance reveals incriminating evidence and the focus of the surveillance becomes the collection of evidence for criminal prosecution, the information may then be submitted to a federal magistrate who is more than capable of determining if there exists the requisite probable cause to continue the

188. 50 U.S.C. § 1804(a)(7)(B) (Supp. 2005).
189. *See supra* Part IV.

surveillance.[190] Although foreign intelligence gathering inevitably will reveal criminal activity, there should not be a criminal prosecutorial purpose in the motivations for conducting FISA approved surveillance.[191]

In addition to amending the degree of foreign intelligence gathering required to secure a FISA order for surveillance, for FISA approved surveillance to be considered a reasonable search within the Fourth Amendment, Congress must clarify what types of activities pose a threat to and are included in "national defense." By defining appropriate targets of foreign intelligence surveillance as those which relate to "the national defense or the security of the United States,"[192] FISA did not sufficiently define those activities which are considered a threat to national defense. Further clarification of these activities is required to ensure that the government may not use FISA to investigate domestic criminal activities which an executive official certifies is a threat to the safety of the nation.[193] Failure to distinguish between threats to the

---

190. However, the problem with this proposed remedy is establishing when the investigation changes to the collection of evidence for criminal prosecution and determining who is to judge when such evidence must be submitted to a magistrate to establish probable cause of the commission of a crime. Were the executive branch to be charged with the duty of determining if the surveillance changes from solely foreign intelligence gathering to criminal prosecution and if a warrant is required, incentive to encourage the executive to not be truthful and submit such information to a magistrate would be the looming rejection and exclusion of information from prosecution where the magistrate determines that the executive submitted the information for a warrant after the focus of the surveillance became criminal prosecution. This deterrent would encourage the executive to be overly cautious and apply for a warrant even earlier than required.

191. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980). In *Truong*, the defendants, in appealing their case and contesting the constitutionality of the warrantless electronic surveillance used, proposed that the executive should only be permitted to conduct such surveillance where the purpose is "solely" for foreign intelligence or policy reasons. *Id.* The *Truong* court rejected this proposal by declaring that the

> "solely" test is unacceptable, however, because almost all foreign intelligence investigations are in part criminal investigations. Although espionage prosecutions are rare, there is always the possibility that the targets of the investigation will be prosecuted for criminal violations. Thus, if the defendants' "solely" test were adopted, the executive would be required to obtain a warrant almost every time it undertakes foreign intelligence surveillance, and, as indicated above, such a requirement would fail to give adequate consideration to the needs and responsibilities of the executive in the foreign intelligence area.

*Id.* at 915-16.

Admittedly, the solely test would impose a significant barrier on the executive and dangerously burden the ability of the government to prevent terrorist threats from a foreign agent. However, in light of the hundreds of misrepresentations made by the executive to the FISA court in applying for FISA orders, see Part VI.D, perhaps such a burdensome requirement on the executive would force compliance with the legally required procedures.

192. 50 U.S.C. § 1801(e)(2)(A) (2000).

193. This problem is further complicated by the FISA court's deference to the executive official that the purpose of the surveillance is for foreign intelligence information which implicates

national defense from a foreign power or its agent and domestic criminal activity permits FISA to be used to investigate ordinary criminal activities by Americans where the executive officials assert that they have a connection with a foreign power.[194]

Along with the required substantive changes to FISA, procedural amendments are also required to ensure that FISA will not be used to escape the Fourth Amendment. As discussed in Part III, the FISA court currently defers to the executive official's assertion that the significant purpose of surveillance is for foreign intelligence purposes, absent a determination that such certification is "clearly erroneous." To properly ensure that the government's purpose is foreign intelligence surveillance, rather than defer to the executive official, the determination of whether the proper purpose of the surveillance is foreign intelligence gathering should be made through a factual inquiry and review by a FISA court judge of the evidence and sworn affidavit submitted by the executive attesting to the existence of probable cause to believe that the target of surveillance has a connection with a foreign power. Although such review by the court may delay the granting of a FISA order for surveillance, this policy would do more to ensure the validity of the executive's assertions than the current procedures. This procedural safeguard is especially necessary in light of the recent disclosure that "the FBI has repeatedly submitted inaccurate information to the Foreign Intelligence Surveillance Court ("FISC") in its efforts to obtain secret warrants in terrorism and espionage cases—severely undermining the Government's credibility in the eye of the Chief Judge of that Court."[195] However, the problem with such a procedural change, in addition to dramatically slowing down the government's ability to respond to and effectively counter threats to national security, lies in the fact that the information before the FISA court was submitted by the executive

---

a threat to the safety of the country.

194. While a definition of what is included in the "national defense or the security of the United States" would limit the executive's ability to abuse the privileges of FISA authorized surveillance, such a definition may be impractical. As we live in an age where technology changes and is invented by the hour, the government, in defining this phrase, would undoubtedly not be able to foresee all those activities which may pose a threat to national security. Perhaps the best solution, rather than defining what threatens the defense or security of the nation, is to continue to have a judge review the evidence submitted by the executive branch to determine if, in the judge's learned opinion, such evidence does pose a threat to the defense or security of the nation. However, the problem comes full circle as a judge cannot interpret the law if there is no law or definition to guide such a decision.

195. *Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. (2007) (statement of Senator Patrick Leahy, Chairman, Committee on the Judiciary), *available at* http://judiciary.senate.gov/member_statement.cfm?id=2569&wit_id=2629 [hereinafter Statement of Senator Patrick Leahy].

branch, and the court, as it is not in the business of collecting facts, has no way to verify that the submitted facts are true. Though this procedural amendment would delay counterintelligence efforts and place the court in an unfamiliar role, such a policy would conclusively ensure that the government has a proper purpose for surveillance.

### *B. The Disclosure Issue*

Currently, 50 U.S.C. § 1806(e) permits any person against whom FISA acquired information is or has been introduced in a criminal prosecution, to make a motion to "suppress the evidence obtained or derived from such electronic surveillance on the grounds that—(1) the information was unlawfully acquired; or (2) the surveillance was not made in conformity with an order of authorization or approval."[196] However, the acquired information is reviewed *in camera* and *ex parte* by the court and the evidence is disclosed to the defendant only where "such disclosure is necessary to make an accurate determination of the legality of the surveillance."[197] As asserted by the D.C. Circuit Court of Appeals in *United States v. Belfield*, disclosure of FISA acquired information may only occur where, upon initial review by the FISA court, the legality of the surveillance may have been complicated by "indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, calling into question compliance with the minimization standards contained in the order."[198] The *Belfield* court further clarified that the rarity of such disclosures to the targets of FISA surveillance is appropriate in light of the delicate and sensitive nature of foreign intelligence information.[199]

While the interest of the government in maintaining secrecy regarding foreign intelligence gathering tactics is certainly valid, it cannot outweigh the interest in ensuring that a defendant receives a fair trial and is informed of the accusations against him, as guaranteed by the Sixth Amendment.[200] In *Belfield*, the court opined that the privacy rights

196. 50 U.S.C. § 1806(e) (2000).

197. *Id.* § 1806(f).

198. United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982) (internal citations omitted).

199. *Id.* The *Belfield* court also pointed to the Supreme Court's statement in *Taglianetti v. United States*, proclaiming that "full disclosure[s] were not necessarily required 'for every issue raised by an electronic surveillance.' . . . To the contrary, such protection will not be required when the task is such that *in camera* procedures will adequately safeguard the 'aggrieved party's' constitutional rights." *Id.* at 149 n.38 (quoting Taglianetti v. United States, 394 U.S. 316, 317 (1969)).

200. U.S. CONST. amend. VI (guaranteeing that "[i]n all criminal prosecutions, the accused shall enjoy the right to . . . be informed of the nature and cause of the accusation").

of the individual, though not protected through mandatory disclosure of the evidence against him, were protected through the procedural oversight of FISA surveillances provided by the three branches of government.[201] However, in light of the numerous procedural and substantive flaws in FISA discussed in Part V and the factual misrepresentations made by the FBI in FISA applications, the current procedural oversight is ineffective in protecting the privacy interests of Americans and permits the abuse of FISA surveillances.[202]

To remedy these issues, two possible solutions are available to the government. The first option is for Congress to amend FISA to ensure that the DOJ cannot use FISA surveillances as a means to escape the Fourth Amendment. Such amendments should include the reestablishment of the primary purpose standard or establishment of the sole purpose standard, defining those crimes which threaten national security, and allowing the FISA court to review the facts in the FISA order application to verify the connection with a foreign agent. The second option available is for an amendment to FISA bestowing upon every defendant prosecuted based on evidence obtained through FISA surveillances the ability to review the information used against him or her. Currently the law gives a FISA judge discretion to allow defendants to view the evidence against them.[203] By revoking the judge's discretion to disclose the information to the defendant and allowing for the evidence to be presented to the defendant upon the making of such a motion to disclose, the defendant would be able to make an informed challenge to the legality of the FISA surveillance against him, thereby protecting the integrity of the criminal justice system and discouraging wrongful convictions. To ensure that such an amendment will not create an unnecessary threat to national security, further procedures should be

---

201. *Belfield*, 692 F.2d at 148.

202. Even more persuasive are the statements made by the court in *Mayfield* regarding disclosure of collected evidence to targets of FISA surveillances:

> Except for the investigations that result in criminal prosecutions, FISA targets never learn that their homes or offices have been searched or that their communications have been intercepted. Therefore, most FISA targets have no way of challenging the legality of the surveillance or obtaining any remedy for violations of their constitutional rights.

Mayfield v. United States, 504 F. Supp. 2d 1023, 1039 (D. Or. 2007).

203. 50 U.S.C. § 1806(f) (2000). The court may

> review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

*Id.*

imposed to ensure that only the defendant and his attorney are able to review the evidence, and then only in a secure room from which the materials may not be removed. Additionally, any information revealing procedures and conduct of the government, not including the specific information acquired, which is not available to the public, should be redacted and not made available to the defendant.

The law should also be amended to give standing to any persons who have been overheard by FISA surveillance, or have a reasonable suspicion that they were overheard, to challenge the surveillance techniques and the evidence submitted to the FISA court in the application for FISA surveillance.[204] Such persons should be given an implied right of action to sue the government for infringing their right to privacy where the evidence submitted to the government was not sufficient to establish probable cause that the target of the surveillance had a connection with a foreign power. The burden of proof would be on the individual to disprove the government's evidentiary support for the FISA surveillance.

Complicating this proposed remedy, in addition to the fact that targets will not know that they are under investigation, is the state secrets privilege which allows the government to refuse disclosure of military and state secrets which, if exposed, pose a reasonable danger of threatening the safety of the nation.[205] The state secrets doctrine is an evidentiary privilege which may be invoked by the executive branch to protect military and state secrets from disclosure in a judicial proceeding.[206] The privilege is only available to the executive and may be invoked only where the court is satisfied that disclosure of evidence or a response to a question will have a negative effect on national security.[207] In accordance with the Classified Information Procedures Act of 1980 ("CIPA"), a court reviewing information determined by an executive order to "require protection against unauthorized disclosure for reasons of national security" may authorize the government to "delete specified items of classified information from documents to be made available to the defendant through discovery."[208] Since CIPA was enacted by Congress, it can certainly be amended to allow defendants challenging FISA surveillance to review the evidence against them.

---

204. *See Mayfield*, 504 F. Supp. 2d at 1039. As mentioned earlier, under the current state of the law, the majority of FISA targets have no way of knowing if they have had surveillance conducted upon their persons or property, unless the investigation results in criminal prosecution. *See supra* note 202.

205. *See, e.g.*, United States v. Reynolds, 345 U.S. 1, 10 (1953).

206. *See, e.g.*, Sterling v. Tenet, 416 F.3d 338, 341 (4th Cir. 2005).

207. *Id.* at 343.

208. Classified Information Procedures Act , 18 U.S.C. app. §§ 1, 4 (2000).

However, it is unclear if Congress has the authority to revoke the state secrets privilege of the executive branch. If this privilege is an inherent power of the executive branch, Congress will not be able to amend the practice and defendants contesting FISA will not be able to review the evidence against them where the state secrets doctrine is invoked. Congress could, however, enact legislation which mandates that in a challenge to FISA surveillance the executive branch may invoke the state secrets privilege only if the government pays damages to the defendant, regardless of the outcome of the case. If the government does not wish to pay damages, the evidence against the defendant must be disclosed. While this policy would provide defendants with a remedy, it is unclear if such a coercive measure against the executive branch in the field of foreign affairs and national security would withstand judicial scrutiny as it may violate the separation of powers doctrine. If the state secrets privilege is determined by a court to be an inherent power of the President and the executive branch, there is little Congress could do to force the President's hand regarding matters strictly delegated to the executive branch by the Constitution.

### *C. Regulations for the Wall*

Although the Patriot Act effectively removed the wall between criminal and intelligence agents and expressly permitted such communications by adopting the significant purpose language, further action by the DOJ is required to ensure that future departmental policies and procedures will not resurrect the wall. To achieve this goal, the current Attorney General must issue regulations, published in the Federal Register, which would formally adopt the proper procedures allowing the permissible degree of communications between the Criminal Division and the FBI in the course of FISA surveillances. Below is a proposed regulation to meet these goals:

"*FISA Communications*—Under the amended Foreign Intelligence Surveillance Act ('FISA'), 50 U.S.C § 1806(k)(1) permits Foreign Intelligence Officials within the Federal Bureau of Investigation ('FBI') conducting FISA surveillances to consult with Federal Law Enforcement Officers within the Department of Justice ('DOJ') to coordinate efforts to investigate plots for international terrorist acts and clandestine intelligence activities by a foreign power or by an agent of a foreign power.

Foreign Intelligence Officials shall have full and exclusive authority for directing and controlling surveillances authorized by the

FISA court, in accordance with the amended provisions of FISA, arising out of a perceived threat to the United States from a foreign power or its agents.

In particular, Foreign Intelligence Officials shall have full and exclusive authority with respect to the above matters for:

Presenting evidence and applications to the FISA court to receive approval for the proposed surveillance;

Reviewing all evidentiary materials and ensuring their accuracy prior to presentation to the FISA court;

Establishing the targeted persons and places of FISA surveillance to collect information which will prevent possible terrorist threats upon the country;

Consulting with Federal Law Enforcement Officers regarding the scope of surveillance and the manner in which the surveillance is to be conducted;

Coordinating and directing all authorized FISA surveillances;

Determining if the collected information warrants criminal prosecution or immediate counterterrorism measures to prevent an imminent threat;

Upon a determination that immediate action is required to counter a terrorist threat, alerting the appropriate military counterterrorism forces to extinguish the perceived threat;

Coordinating with the appropriate military officials to determine the appropriate timing and methods to combat terrorist threats;

Upon determination that criminal prosecution is necessary to impede a terrorist threat, submitting all information acquired pursuant to FISA to Federal Law Enforcement Officers for approval by a Federal Magistrate regarding the existence of probable cause to collect further evidence of criminal activity by the targeted individual(s).

*Restrictions*—Under no circumstances, prior to the determination by Foreign Intelligence Officials that criminal prosecution is necessary, shall Federal Law Enforcement Officers be permitted to direct or control a FISA authorized surveillance.

Foreign Intelligence Officials may coordinate and consult with Federal Law Enforcement Officers regarding FISA surveillance, taking under advisement the suggestions of Federal Law Enforcement Officers. Under no circumstances may the final determination regarding the techniques used, the individuals targeted, or the information retained in the course of FISA surveillance be made by Federal Law Enforcement Officers.

*Responsibilities of the Director of the FBI*—Concerning FISA authorized surveillances, the Director of the FBI is charged with the

responsibility of ensuring that the level of communication between Foreign Intelligence Officials and Federal Law Enforcement Officers does not amount to the Federal Law Enforcement Officers directing or controlling FISA surveillance.

It is the duty of the Director of the FBI, in consultation with the agents in charge of the FISA surveillance, to determine if military action or criminal prosecution is necessary to most effectively counter the terrorist threat.

It is the duty of the Director of the FBI to ensure that, upon determination that criminal prosecution is proper, the information acquired pursuant to FISA is transferred to the Assistant Attorney General, Criminal Division.

*Responsibilities of the Assistant Attorney General, Criminal Division*—Upon receipt of FISA acquired information from the Director of the FBI, it is the duty of the Assistant Attorney General to ensure that the evidence acquired is submitted to the appropriate Federal Magistrate for a probable cause determination to continue surveillance of the target.

Upon determination by a neutral and detached magistrate of proper probable cause of criminal activity, the Assistant Attorney General may oversee the continued surveillance of the target.

*Duration of Investigations*—The Director of the FBI will carry out these responsibilities until such time as, in his judgment, further FISA surveillance is no longer necessary. The Assistant Attorney General, Criminal Division will carry out these responsibilities until such time as, in his judgment, collection of evidence for criminal prosecution is no longer required."

The proposed regulation would ensure that the wall created by the DOJ could not be resurrected in the future, in addition to ensuring that the level of communication between Foreign Intelligence Officials and Federal Law Enforcement Officers will be effective and legal.

### *D. Recent Developments*

Despite the minimal standard of proof required to secure a FISA order for surveillance, the executive branch has consistently abused the FISA application process by misrepresenting factual assertions in FISA applications to the FISA court and disregarding the FISA process entirely.[209] In 2005, Attorney General Alberto Gonzales conducted a press briefing in which he admitted to a program authorized by the

209. *See* A REVIEW OF THE FBI, *supra* note 121, at 36-37.

President whereby electronic communications were intercepted without a warrant or a FISA order where one party to the communication was outside the United States.[210] The Attorney General asserted the program was legal, as Congress's Authorization of Use of Military Force ("AUMF"), constituted "authorization . . . to engage in this kind of signals intelligence."[211] Without judging the legality of the executive branch's assertion regarding the legality of the surveillances under the AUMF, such action demonstrates the executive branch's willingness to bypass congressionally imposed limitations on warrantless surveillance.

In June 2006, the Office of the Inspector General ("OIG") of the DOJ released a report reviewing the FBI's intelligence procedures related to the attacks on September 11, 2001.[212] In this report, the OIG disclosed the fact that between 2000 and 2001, the FISA court became aware of approximately one hundred factual errors contained in FISA applications submitted by the FBI.[213] The report highlighted the fact that nearly seventy-five of these errors related to the targets of FISA surveillance and their asserted connections with foreign powers or terrorist organizations.[214] In addition to these factual inaccuracies, the report also noted that "contrary to what had been represented to the FISA Court, agents working on criminal investigation had not been restricted from the information obtained in the intelligence investigation."[215]

In March 2007, another report was filed by the OIG concerning factual misrepresentations by the FBI regarding the foreign intelligence surveillance technique known as National Security Letters ("NSL").[216] This report cited numerous abuses by the FBI in its NSL program, including obtaining information concerning the wrong person, retaining information not sought in the application for a NSL, and continuing to retrieve information beyond the time period referenced in the NSL, in addition to a number of other violations.[217] Though this report did not

---

210. Press Briefing, Alberto Gonzales, Att'y Gen. & Gen. Michael Hayden, Principal Deputy Dir. for Nat'l Intelligence (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html.

211. *Id.*; *see also* Pub. L. No. 107-40, § 2(a), 115 Stat. 224, 224 (2001) (giving the President the authority to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001").

212. A REVIEW OF THE FBI, *supra* note 121.

213. *Id.* at 36.

214. *Id.*

215. *Id.* at 37.

216. U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (2007).

217. *Id.* at 31-36.

concern FISA applications, it established a patterned history of misrepresentation and abuse of power by the FBI concerning foreign intelligence surveillance.

Only a few weeks after the March 2007 OIG report was released, the *Washington Post* broke a story regarding the continued abuse by the FBI of the FISA system.[218] The article claimed the FBI submitted factual inaccuracies to the FISA court in their applications for FISA surveillances ranging from misrepresentations about a target's familial relationships to "citing information from informants who were no longer active."[219] The same day this story was published, the Senate Committee on the Judiciary conduced a hearing on FBI oversight. Chairman Patrick Leahy, in addition to noting the *Washington Post* article, the NSL issue, and FISA application misrepresentations, proclaimed:

> This pattern of abuse and mismanagement causes me, and many others on both sides of the aisle, to wonder whether the FBI and Department of Justice have been faithful trustees of the great trust that the Congress and American people have placed in them to keep our Nation safe, while respecting the privacy rights and civil liberties of all Americans.[220]

To remedy these noted abuses, Senator Leahy recommended more effective congressional oversight, in addition to the increased FBI resources and tools to effectively conduct its domestic counterterrorism measures.[221] Though the Senator's suggested remedies would help to resolve the problem, due to the recurrence of the FBI's abuse of power, congressional oversight alone is not a sufficient remedy. To permanently resolve the issues noted, further procedural safeguards, such as those suggested in Part VI.A, are required to ensure that the FISA court operates as an intrusive and thorough check of the FBI's FISA applications rather than a rubber stamp for the abuse of American's civil liberties.[222]

---

218. John Solomon, *FBI Provided Inaccurate Data for Surveillance Warrants*, WASH. POST, Mar. 27, 2007, at A5.

219. *Id.*

220. Statement of Senator Patrick Leahy, *supra* note 195.

221. *Id.*

222. *See* Letters from William E. Moschella, Assistant Att'y Gen., to L. Ralph Mecham, Dir., Admin. Office of the U.S. Courts, Dennis Hastert, Speaker, U.S. House of Representatives, Richard Cheney, President, U.S. Senate (Apr. 28, 2006), *available at* http://www.usdoj.gov/nsd/foia/reading_room/2005fisa-ltr.pdf (stating that in 2005, 2,074 FISA applications were submitted to the FISA court and 2,072 of those were approved by the court).

### *E. Proposed Legislation*

Recognizing the need for change, Congress, with input from the Administration, has proposed legislative amendments to FISA to ensure that FISA is "the exclusive means by which electronic surveillance . . . may be conducted"[223] and to update surveillance techniques in light of technological advancements in communications "while continuing to protect the privacy interest of persons located in the United States."[224]

Congress recently passed the Protect America Act of 2007, intended to amend FISA "to provide additional procedures for authorizing certain acquisitions of foreign intelligence information."[225] This law clarifies that the definition of "electronic surveillance" under FISA does not encompass surveillances directed at persons located outside the United States.[226] The law further modernizes FISA by allowing the executive branch to conduct warrantless surveillance without FISA court approval where the target of surveillance is located in a foreign country, permitting the Attorney General to direct a third-party to provide the government with "information, facilities, and assistance" to obtain the desired electronic surveillance information, and requiring the Attorney General to submit to the FISA court those procedures used to collect information about non-U.S. persons located in a foreign country to ensure that the target is outside the United States.[227] Although the law ensures surveillance techniques towards foreign persons outside of the United States are properly conducted, there remains the possibility for FISA surveillances to be misused against persons within the United States.

An amendment to FISA proposed by the Senate, the Foreign Intelligence Surveillance Improvement and Enhancement Act of 2007, which has sat in committee untouched since April 16, 2007, provides for increased reporting by the President to Congress on the use of electronic surveillance for foreign intelligence purposes toward United States persons, mandatory Supreme Court review of the Terrorist Surveillance

---

223. Foreign Intelligence Surveillance Improvement and Enhancement Act of 2007, S. 1114, 110th Cong. § 101(a) (2007).

224. Press Release, U.S. Dep't of Justice, Fact Sheet: Title IV of the Fiscal Year 2008 Intelligence Authorization Act, Matters Related to the Foreign Intelligence Surveillance Act (Apr. 13, 2007).

225. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (to be codified at 50 U.S.C. §§ 1803, 1805).

226. *Id.* § 2; *see also* Press Release, The White House, Fact Sheet: The Protect America Act of 2007: President Bush Signs Legislation Modernizing Foreign Intelligence Law to Better Protect America (Aug. 6, 2007).

227. Protect America Act of 2007 § 2.

Program, which permits warrantless surveillance of international communications into and out of the United States, emergency surveillance measures whereby intelligence agents may conduct warrantless surveillance without prior court approval where the agent's superior determines an emergency situation exists, development of a document management system to improve the efficiency and efficacy of communications between the DOJ, FBI, and FISA court, and increased personnel within DOJ, FBI, FISA court, and the National Security Agency.[228] The bill also mandates that any application for a FISA order must be accompanied by facts particular to the individual who is to be the target of surveillance.[229] Although this bill would create a more efficient flow of information, improve the accuracy of information included in a FISA application, and increase oversight of executive branch foreign intelligence surveillance programs, it falls short of the changes required to ensure the executive branch is unable to abuse its power in this area.

Another proposed amendment to FISA, the Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act of 2007, was introduced by the House of Representatives on November 9, 2007.[230] Concerning the actual procedures authorized under FISA, the proposed legislation focuses on amending the ability of the government to conduct warrantless surveillance on non-United States persons located outside the United States while failing to address the procedures for those United States persons with a connection to a foreign agent located within the United States.[231] On a positive note, the proposed amendments would require quarterly audits submitted to Congress by the DOJ's Inspector General regarding any information concerning United States persons within the United States acquired through warrantless surveillance, an increase in the number of FISA court judges from eleven to fifteen, require the Attorney General to improve documentation and record keeping of FISA surveillance and applications, and mandate the President to report to congressional committees on any foreign intelligence surveillance program in existence since September 11, 2001 which involves the electronic surveillance of a United States person.[232] The amendments would also

228. Foreign Intelligence Surveillance Improvement and Enhancement Act of 2007, S. 1114, 110th Cong. §§ 103, 104(a), 202(g)(1)(B), 204(a), 205 (2007).

229. *See id.* § 302.

230. Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act of 2007, H.R. 3773, 110th Cong. § 1(a) (2007).

231. *Id.* §§ 2-3.

232. *Id.* §§ 5, 7, 14(a), 16.

give the President the power to disregard the FISA procedures and conduct warrantless electronic surveillance where Congress has declared war, issued an authorization for the use of military force, or is unable to convene due to an attack on the United States.[233] These amendments would increase the executive's accountability for failures to comply with federal law, however, they do not remedy the numerous lingering problems with FISA.

While both Congress and the Administration have recognized the need for changes in the FISA surveillance system, the proposed amendments do not go far enough to protect the privacy interests of Americans. In particular, the proposed amendments do not allow defendants to view upon demand FISA-collected evidence being used to convict them, it does not properly distinguish between national security and domestic criminal activities which may be targeted by FISA surveillances, and it fails to impose appropriate safeguards to ensure that the information used in a FISA application is accurate. The amendments should focus less on the surveillance measures used on non-United States persons outside the United States and more on those used against United States citizens located in the United States.

## VII. CONCLUSION

Although the President has the inherent powers to conduct foreign affairs and protect against threats to the security of the nation, such powers cannot be exerted in a manner which conflicts with other provisions of the Constitution. In its current form, as amended by the Patriot Act, FISA not only impermissibly infringes on the privacy rights of Americans, it authorizes surveillance in violation of the constitutional requirements for warrantless surveillance for foreign intelligence purposes established by the court in *Truong* and the Fourth Amendment balancing test applied in the *Keith* decision. The Patriot Act provides the government with effective tools to prevent future terrorist acts, however, the incredible deference given to the DOJ in applying for a FISA order, the ability to use FISA to investigate criminal activity with a minimal connection to a foreign agent, the lack of appropriate congressional and judicial oversight, the inability of targets of FISA surveillance to challenge the law, and the general infringement on the privacy interests of Americans permitted by the Patriot Act amendments so significantly outweigh the government's interest in national security as to make the Act unconstitutional. In particular, Congress must articulate or the courts

233. *Id.* § 9.

must clarify those activities which are included in a threat to the "national security." Failure to appropriately limit this phrase permits the executive branch to escape a demonstration of probable cause of criminal activity where it has certified that a foreign agent poses a threat to national security.

The Patriot Act amendments to FISA were a predictable and necessary response to the attacks of September 11th. Few will argue that the intelligence community did not need restructuring after its failure to detect and deter these attacks. However, the safety of the nation must not blind the Administration and Congress to the threat to the civil liberties of Americans created by the authorized programs. Although action was required to remove the wall preventing communications within the DOJ, the Patriot Act amendments to FISA were not the constitutional means to achieve this end. In addition to the suggested legislative and regulatory amendments, the Supreme Court must review the amendments to FISA and should affirm the *Mayfield* court's decision, declaring that in its current state, FISA provides too much deference to the executive and authorizes a surveillance program in violation of the Fourth Amendment and the constitutionally mandated primary purpose standard.

*Joshua H. Pike**

* I would like to thank Professor Eric M. Freedman for his guidance and advice in the writing process. I would also like to thank the managing editors of the *Hofstra Law Review*, Renato D. Matos, Kathleen Dreyfus Bardunias, and Irina Boulyjenkova, and Rebecca Kulik, my Note editor, for putting up with my multitude of questions and errors. I would finally like to thank my parents, siblings, and friends for their constant support and encouragement in this endeavor. I would like to dedicate this Note to my late grandfather, Frank R. Pike, for being an inspiration and guiding light throughout my life. It was his fighting for this country which provided me with the freedom and courage to address this controversial issue.