Vanderbilt Law Review

Volume 58 | Issue 5 Article 6

10-2005

The Revamped FISA: Striking a Better Balance Between the Government's Need to Protect Itself and the 4th Amendment

J. Christopher Champion

The Revamped FISA: Striking a Better Balance Between the Government's Need to Protect Itself and the 4th Amendment

I. INTRODUCTION

The investigations of the 9/11 terrorist attacks highlighted a series of lapses in intelligence-sharing within the federal government regarding terrorist operations. One area closely examined by Congress,[1] the judiciary,[2] and many legal and political commentators[3] is the appropriate scope of intelligence collection within the United States "concerning foreign threats to the nation's security" ("foreign intelligence").[4] Domestic intelligence collection is a particularly complex sphere of national security as gathering intelligence on American soil requires balancing the privacy rights of individuals guaranteed by the Fourth Amendment against the nation's need to protect itself.

The Foreign Intelligence Surveillance Act of 1978 ("FISA") governs the conduct of electronic surveillance and physical searches carried out for foreign intelligence purposes within the United States.[5] FISA establishes procedures for collecting foreign intelligence information, which are parallel to, and independent of, the conventional law enforcement channels used to secure judicial approval for searches and electronic surveillance.[6] Under FISA, federal investigators submit applications for foreign intelligence surveillance to a secret court that exists for the sole purpose of reviewing government requests to gather information pursuant to the statute.[7]

Prior to 2002, the courts (including the FISA court) only authorized searches and/or surveillance under FISA where collecting foreign intelligence information was the "primary purpose" of the investigation.[8] This primary purpose test was intended to facilitate the collection of foreign intelligence and limit the use of FISA as an

---

1. *E.g.*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter Patriot Act].

2. *E.g.*, *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d. 611 (Foreign Intelligence Surveillance Ct. 2002).

3. *E.g.*, Craig S. Lerner, *The USA Patriot Act: Promoting the Cooperation of Foreign Intelligence Gathering and Law Enforcement*, 11 GEO. MASON L. REV. 493 (2003).

4. For the purposes of this Note, "foreign intelligence" includes any information concerning threats to the nation's security from abroad. Such information may concern foreign governments or terrorist organizations composed mainly of foreign nationals. This category specifically excludes information regarding United States citizens or groups composed thereof.

5. 50 U.S.C. §§ 1801-71 (2004).

6. *Id.*

7. 50 U.S.C. § 1803 (2004).

8. *E.g.*, United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984).

end-run around obtaining a normal search warrant.[9] Enforcing the primary purpose test required courts to discern whether an investigation was conducted primarily for intelligence collection or for law enforcement purposes.[10] Repeated judicial inquiries into the motives behind FISA investigations eventually led the Justice Department to establish formal procedures for handling FISA information to ensure that such investigations were not being used to pursue criminal targets.[11]

After the 9/11 attacks, the Patriot Act amended several sections of FISA.[12] Most notably, the Patriot Act allows FISA investigations where collecting foreign intelligence is a "significant purpose" of the collection effort.[13] In 2002, the reach of FISA was expanded even further when the FISA Court of Review struck down the primary purpose test altogether.[14] After this decision, the government could collect foreign intelligence for use as evidence in a criminal prosecution.[15]

The new FISA regime shifts surveillance requests away from the Fourth Amendment scrutiny of Article III judges and into the hands of the Justice Department and the secret FISA tribunal. Concededly, balancing the government's need to protect the country from further terrorist attacks with the Fourth Amendment's guarantee of privacy is not an easy task. A new FISA regime that incorporates the Patriot Act amendments need not, however, discard twenty-five years of judicial analysis regarding the proper role of FISA-derived evidence in criminal prosecutions. It is essential that courts rethink the primary purpose doctrine in a manner that effectuates the Patriot Act's purpose of ensuring better intelligence-sharing.

Part II of this Note describes the evolution of the executive power to collect foreign intelligence from the earliest days of the

---

9. *See* United States v. Truong, 629 F.2d 908, 915-16 (4th Cir. 1980) (discussing the importance of granting the executive sufficient discretion to fulfill its responsibility to collect foreign intelligence).

10. *See id.* (rejecting a test in which the government's sole purpose for the investigation was to gather foreign intelligence because "[a]lmost all foreign intelligence investigations are in part criminal investigations").

11. *See generally* Memorandum from Attorney General Janet Reno to the Assistant Attorney General, Criminal Division (July 19, 1995), *available at* http://www.fas.org/irp/agency/doj/fisa/1995procs.html [hereinafter Reno memorandum].

12. *E.g.*, Patriot Act, *supra* note 1, §§ 206, 207, 215, 218.

13. 50 U.S.C. § 1804(a)(7)(B) (2004).

14. *In re* Sealed Case, 310 F.3d 717, 727 (Foreign Intelligence Surveillance Ct. of Review 2002).

15. *Id.*

Republic through the Congressional response to 9/11. Part III analyzes the decision of the FISA Court of Review to interpret the original 1978 FISA statute so broadly as to render unnecessary the changes implemented by Congress in the Patriot Act. Part IV proposes that courts should closely scrutinize government attempts to introduce FISA-derived evidence in criminal prosecutions. Such scrutiny is necessary because the present system inadequately protects individuals from unreasonable searches, as guaranteed by the Fourth Amendment.

II. BACKGROUND

A. The Historical Power of the President to Collect Information Regarding Threats Posed by Foreign Powers

Despite the Fourth Amendment's command that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated,"[16] for much of the nation's history, courts have allowed the executive branch to exercise near absolute power in the collection of information regarding foreign threats.[17] The willingness to bypass Fourth Amendment scrutiny is grounded in the notion that subjecting the government to the probable cause standard needed to obtain a criminal warrant could "unduly frustrate the efforts of Government to protect itself."[18] Constitutional support for such power to enact unfettered surveillance in the pursuit of foreign intelligence information derives from the executive's designation as "the pre-eminent authority in [the conduct of] foreign affairs."[19] In a case involving executive surveillance of a domestic threat to the government, the Supreme Court noted that

> the President of the United States has the fundamental duty, under Art. II, § 1, of the Constitution to "preserve, protect and defend the Constitution of the United States." Implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means. In the discharge of this duty, the President . . . may find it necessary to employ electronic surveillance to obtain

16. U.S. CONST. amend. IV.

17. William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 2 (2000).

18. United States v. United States Dist. Court, 407 U.S. 297, 315 (1972).

19. United States v. Truong, 629 F.2d 908, 914 (4th Cir. 1980).

> intelligence information on the plans of those who plot unlawful acts against the Government.[20]

The different standards applied to the government's attempts to procure intelligence information and information on criminal activity can be explained by the different means of obtaining the two types of information as well as the information's ultimate use. Compared to investigating violations of criminal law, collecting foreign intelligence information requires an extreme degree of secrecy.[21] Further, with few exceptions, the ultimate goal of foreign intelligence collection is the protection of U.S. interests, not the criminal prosecution of the individuals targeted for search or surveillance.[22] These differences led the Supreme Court to acknowledge that the requirements for traditional criminal warrants might not be applicable in the counter-intelligence context.[23]

The history of government involvement in intelligence matters can be traced to the early days of the Revolutionary War, when the Continental Congress established the Committee for Secret Correspondence.[24] President George Washington had significant experience managing military intelligence operations during the Revolutionary War.[25] Accordingly, after taking office, he sought to centralize the collection of information within the executive branch.[26] In his first State of the Union address, Washington specifically requested an appropriation for intelligence operations and Congress complied.[27] Most early Presidents followed Washington's example by closely guarding the specifics of intelligence collection at home and abroad.[28] In response to strong executive action in initiating and

---

20. *United States Dist. Court*, 407 U.S. at 310.

21. *See id.* at 319 (noting that "secrecy is the essential ingredient in intelligence gathering") (internal citation omitted).

22. *See id.* at 318-19 (noting that the government contended courts should not apply Fourth Amendment standards to foreign intelligence operations because they are almost never meant to gather evidence for criminal prosecutions).

23. *See United States Dist. Court*, 407 U.S. at 322. ("We recognize that domestic security surveillance may involve different . . . considerations from the surveillance of 'ordinary crime.'"). For instance, information collected by the executive branch regarding the actions of foreign intelligence services and terrorist organizations would be of little value if the collection target had to be notified of a search prior to or commensurate with its execution. Banks & Bowman, *supra* note 17, at 5. The Court's observation regarding counter-intelligence is clearly dicta, since the case before it concerned the collection of information about purely domestic threats to national security.

24. Banks & Bowman, *supra* note 17, at 10-11.

25. *Id.* at 15.

26. *Id.*

27. *Id.*

28. *Id.* at 17.

managing covert intelligence activity, Congress generally deferred to the belief that such power was vested in the executive.[29]

The executive branch continued to engage in the type of foreign intelligence collection later authorized by FISA in the years prior to World War I. In 1915, President Woodrow Wilson initiated a surveillance program, administered by the Secretary of the Treasury, which targeted the German and Austro-Hungarian diplomatic corps.[30] Information gleaned from these wiretaps, supplemented with British intelligence, led to the expulsion of several German intelligence officers posing as diplomatic officials.[31]

In the 1920s and '30s, J. Edgar Hoover, the first director of the Federal Bureau of Investigation ("FBI" or the "Bureau"), consolidated the responsibility for domestic intelligence in the Bureau.[32] While the FBI's primary mission was to investigate violations of federal law, it also had a presidential mandate to monitor the activities of groups deemed subversive to the interests of the United States.[33] These intelligence operations were distinct from the FBI's primary mission as they were exclusively defensive in nature and not intended to help prove violations of federal law.[34] The FBI's authority to conduct wide-ranging counter-intelligence operations continued to expand after the conclusion of World War II, when the FBI assumed expanded powers in the name of defending the nation against subversive activity.[35]

The virtually unfettered executive power to collect information related to perceived threats to the government continued relatively unabated until the early 1970s. At that time, Congress began to investigate the extent of violations of individuals' privacy interests by intelligence officials in the United States.[36] The resulting Church Committee Report detailed extensive surveillance of individuals who did not pose a threat to national security.[37] Following these revelations, Congress and the courts undertook a series of steps to provide a more measured constitutional and statutory framework for intelligence collection.

---

29. *Id.* at 18.

30. *Id.* at 19-20.

31. *Id.* at 20.

32. *Id.* at 26.

33. *Id.* at 26-27.

34. *Id.*

35. *Id.* at 28-29.

36. Sharon H. Rackow, Comment, *How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of "Intelligence" Investigations*, 150 U. PA. L. REV. 1651, 1666 (2002).

37. *Id.*

B. Constitutionality of Electronic Surveillance and the Development of the Foreign Intelligence Exception

Prior to the 1967 Supreme Court decision in *Katz v. United States*,[38] electronic surveillance by government officials was not considered a "search or seizure" and thus was exempt from constitutional review.[39] The Court reasoned that electronic surveillance did not constitute a search because it did not require an invasion of physical space belonging to an individual.[40] Furthermore, the Court had previously held that intangible things such as a person's words could not be "seized" in a manner that triggered Fourth Amendment protections.[41]

Katz reflected a shift in Fourth Amendment jurisprudence from the protection of physical space to the protection of individual privacy.[42] The determining factor in whether a search or seizure was entitled to Fourth Amendment protection lay not in the physical location of an object or action, but in the individual's "reasonable expectation of privacy" in that location.[43] Employing this privacy-based reasoning, the Supreme Court in *Katz* held that a listening device attached to the outside of a public phone booth was subject to Fourth Amendment scrutiny when the prosecution sought to introduce evidence gleaned from the wiretap against the defendant.[44] While *Katz* dramatically limited the ability of law enforcement officers and prosecutors to employ wiretaps and other means of electronic surveillance, the decision specifically reserved judgment on the power of executive branch officials to employ electronic surveillance in foreign intelligence operations.[45]

---

38. *See* 389 U.S. 347, 352-53 (1967) (reviewing precedent that previously left electronic surveillance outside of "search" or "seizure").

39. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (reasoning that a telephone wiretap fell outside of a Fourth Amendment analysis).

39. *See id.* at 463-64 (distinguishing cases involving physical entry into a defendant's home or office from the present case where "voluntary conversations" were "secretly overheard" without physical entry into the defendant's property.).

41. *See id.* at 464-66 (reasoning, *inter alia*, that a person meant his words to move outside of his home when he spoke on a telephone because telephone wires and connection equipment existed primarily outside of the confines of his residence).

42. *See* Katz, 389 U.S. at 351 (rejecting the significance of a "constitutionally protected area" in Fourth Amendment analysis and asserting that "the Fourth Amendment protects people, not places").

43. *See id.* at 351-52 ("But what [appellant] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

44. *Id.* at 353-54.

45. *See id.* at 358 n.23 ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.").

Shortly after *Katz*, Congress enacted warrant procedures for the use of electronic surveillance in law enforcement investigations as part of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[46] Title III authorizes law enforcement officers to use electronic surveillance pursuant to a court order[47] in the investigation of a specified list of crimes.[48] The statute provides that judges shall only grant surveillance warrants where "there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense."[49] Surveillance under a Title III warrant is limited to thirty days (although extensions may be granted)[50] and the subject of electronic surveillance must be notified of the surveillance within 90 days of its termination.[51] Like *Katz*, Title III exempted the collection of foreign intelligence from the limits imposed on "normal" electronic surveillance:

> 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. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.[52]

The Court concluded that, while broad in scope, the exception to the normal warrant requirement outlined in § 2511(3) did not apply to warrantless surveillance in domestic security investigations.[53]

In *United States v. United States District Court*, the Supreme Court held that warrantless surveillance of individuals suspected of conspiring to bomb a CIA office in Michigan violated the Fourth Amendment protection against unreasonable search and seizure.[54]

---

46. 18 U.S.C. §§ 2510-22 (2004).

47. Title III also contains an emergency exception that empowers law enforcement officers to establish electronic surveillance under certain conditions. The officers then have 48 hours from initiation of the emergency surveillance to obtain a court order authorizing the surveillance. 18 U.S.C. § 2518(7) (2004).

48. *See id.* § 2516 (listing the offenses where federal officials may apply for a surveillance warrant).

49. *Id.* § 2518(3)(a).

50. *Id.* § 2518(5).

51. *Id.* § 2518(8)(d).

52. *Id.* § 2511(3) (repealed 1978).

53. *See* United States v. United States Dist. Court, 407 U.S. 297, 321 (1972) (holding that the "Government's concerns do not justify departure . . . from the customary Fourth Amendment requirement of judicial approval prior to initiation of . . . surveillance" in a criminal prosecution for bombing a CIA office in Michigan).

54. *Id.*

The Court acknowledged the constitutional duty of the President to "preserve, protect and defend the Constitution of the United States" and noted that various Presidents had authorized warrantless surveillance in the exercise of this duty.[55] However, in balancing the duty of the government to protect domestic security with the danger to individual privacy posed by warrantless searches, the Court determined that, where the threat to security is entirely domestic, "[t]he circumstances . . . do not justify complete exemption . . . from prior judicial scrutiny."[56] Like *Katz* and Title III, the Court specifically disclaimed the possibility that its holding hindered the ability of the executive branch to conduct warrantless surveillance of the activities of foreign powers or their agents.[57]

Lower courts further modified the foreign intelligence exception to Title III's warrant requirement to apply only where the collection of foreign intelligence was the primary purpose of the warrantless wiretap.[58] In *United States v. Truong*, the Fourth Circuit balanced the government's need to collect foreign intelligence information with the rights of an accused when the government seeks to introduce evidence obtained in a foreign intelligence wiretap against an individual in a criminal proceeding.[59] The Fourth Circuit conducted a balancing test similar to the one in *United States District Court*, but concluded that "[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations."[60] Furthermore, the court determined that because the executive requires such flexibility in the execution of its foreign affairs duties, "the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance."[61]

Importantly, the *Truong* court acknowledged that the power of the executive branch to collect foreign intelligence information was

55. *Id.* at 310.

56. *Id.* at 320.

57. *Id.* at 321-22.

58. *See* United States v. Truong, 629 F.2d 908, 915 (4th Cir. 1980) (limiting the application of the foreign intelligence exception to situations where "the object of the search or the surveillance is a foreign power, its agent or collaborators").

59. *See id.* at 912 (identifying the issue before the court as a balance between the "the legitimate need of Government to safeguard domestic security" and "whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant").

60. *Id.* at 913.

61. *Id.* at 914.

subject to the competing privacy interests of the Fourth Amendment.[62] *Truong* involved a prosecution of two U.S. residents (one a U.S. citizen) on espionage charges for passing classified documents to agents of the North Vietnamese government during negotiations to end the Vietnam War.[63] The charges were based on extensive surveillance of the defendants, including a continuous wiretap of defendant Truong's phone for 255 days; however, at no time did the government seek or obtain court authorization for the wiretap.[64]

The Fourth Circuit conducted a functional analysis of the relative competencies of the executive and judiciary branches and determined that, as long as an investigation is focused primarily on the collection of foreign intelligence, warrantless wiretaps are constitutional and can be introduced as evidence in criminal proceedings.[65] When the focus of the investigation turns to a criminal investigation of individual suspects, however, the courts are competent to conduct Title III determinations of whether there exists a sufficient factual basis for the authorization of electronic surveillance.[66] Evidence collected from warrantless wiretaps whose primary purpose was something other than collection of intelligence (*e.g.* to implicate an individual for violating a criminal statute) could not be admitted at trial under the Fourth Amendment.[67]

Applying its new primary purpose test, the Fourth Circuit concluded that the government's investigation of the defendants began as a foreign intelligence operation; however, it transformed into a primarily criminal investigation when the Criminal Division of the Justice Department assumed control of the case from the various intelligence agencies that had initiated the surveillance.[68] The prosecution could therefore properly introduce evidence obtained from the wiretaps before the investigation became primarily law enforcement in nature.[69]

---

62. *Id.* at 915.
63. *Id.* at 911-12.
64. *Id.*
65. *Id.* at 915.
65. *Id.*
67. *Id.*
68. *Id.* at 916.
69. *Id.*

C. FISA Becomes the Modern Approach to Domestic Intelligence Collection

In response to the court decisions identifying a foreign intelligence exception to the Title III warrant requirement and the abuses of that exception uncovered by the Church Committee,[70] Congress enacted the Foreign Intelligence Surveillance Act of 1978.[71] The Act provided a statutory framework for domestic intelligence collection "to insure that electronic surveillance by the U.S. Government within this country conforms to the fundamental principles of the Fourth Amendment."[72]

FISA created two new Article III courts, the Foreign Intelligence Surveillance Court ("FISC") and the Foreign Intelligence Court of Review ("FISA Court of Review" or "Court of Review"), to consider applications by executive branch officials for electronic surveillance operations intended to collect foreign intelligence.[73] The statute directs the FISC to grant surveillance orders where it finds that there is probable cause to believe that "the target of surveillance is a foreign power or agent of a foreign power."[74] The term "foreign power" is defined broadly by the statute and includes foreign governments, factions of foreign nations, and groups "engaged in international terrorism or activities in preparation therefor."[75] The executive official submitting the application must also certify that information sought through the surveillance is not available through normal investigative means and that a significant purpose of the proposed operation is to obtain foreign intelligence information.[76]

---

70. Rackow, *supra* note 36, at 1666.

71. Pub. L. No. 95-511, § 301, 92 Stat. 1782, 1798 (1978).

72. S. Rep. No. 95-604, at 15 (1977), *as reprinted in* 1977 U.S.C.C.A.N. 3904, 3916. While FISA originally dealt exclusively with electronic surveillance, the statute was later amended to permit physical searches to collect foreign intelligence information. The standard and procedure for physical searches pursuant to FISA is the same as those for electronic surveillance. 50 U.S.C. §§ 1822-23 (2004).

73. The Act creates a two-tier system of judicial review for proposed FISA orders. The Foreign Intelligence Surveillance Court (FISC) is composed of 11 federal district judges and hears all applications for surveillance or search orders under FISA. If the FISC denies a proposed order, the government can appeal to the Foreign Intelligence Surveillance Court of Review (Court of Review or FISA Court of Review), which is composed of three federal district or circuit court judges. A denial of a FISA order by the Court of Review can be appealed to the Supreme Court. Appointments to both FISA courts are public and are the exclusive province of the Chief Justice of the United States Supreme Court. 50 U.S.C. § 1803 (2004).

74. *Id.* § 1805(a)(3)(A).

75. *Id.* § 1801(a).

76. *Id.* § 1804. FISA originally required that the executive officer certify that the "purpose" of the surveillance was to obtain foreign intelligence information. The Patriot Act amended this

The requirements for FISA surveillance orders and Title III warrants differ in significant ways pertinent to Fourth Amendment analysis. First, unlike Title III, FISA does not require any showing of probable cause to believe a crime is about to be or has been committed; the probable cause requirement under FISA is limited to establishing a connection between an individual and a broadly defined "foreign power."[77] Second, Title III limits the duration of surveillance warrants (and each subsequent extension) to 30 days,[78] while a single FISA order can permit electronic surveillance for up to one year.[79] Title III also requires that targets of electronic surveillance be notified in writing within 90 days of the termination of the surveillance,[80] whereas under FISA, the targeted party is not entitled to view the application for surveillance even if the evidence ripens into a criminal prosecution.[81]

The use of FISA evidence in criminal prosecutions has been held constitutional under the Fourth Amendment by every court that has considered the issue.[82] While the Supreme Court has not ruled on the constitutionality of FISA-obtained evidence, courts confronting the issue have read the Supreme Court's decision in *United States District Court* to imply that "the warrant requirement is flexible and that different standards may be compatible with the Fourth Amendment in light of the different purposes and practical considerations of domestic national security surveillances."[83] In a recent opinion, the FISA Court of Review compared the requirements for a Title III warrant and a FISA order, concluding that "in many significant respects the two statutes are equivalent" and "to the extent a FISA order comes close to meeting Title III . . . [this] certainly bears on its reasonableness under the Fourth Amendment."[84]

---

section of FISA to allow for surveillance where the collection of foreign intelligence is a "significant purpose" of the surveillance. *Id.*

77. *Id.* § 1805(a)(3)(A).

78. 18 U.S.C. § 2518(5) (2004).

79. 50 U.S.C. § 1805(e) (2004).

80. 18 U.S.C. § 2518(8)(d) (2004).

81. 50 U.S.C. § 1806(f) (2004); *see also* United States v. Duggan, 743 F.2d 59, 67-73 (2d Cir. 1984) (describing the court's in camera review of evidence procured subsequent to a FISA order and the court's decision that the procedures mandated by FISA comport with the Fourth Amendment).

82. *E.g.*, United States v. Cavanagh, 807 F.2d 787, 790-92 (9th Cir. 1987); United States v. Duggan, 743 F.2d 59, 59 (2d Cir. 1984); United States v. Nicholson, 955 F. Supp. 588, 589 (E.D. Va. 1997).

83. *Duggan*, 743 F.2d at 72.

84. *In re* Sealed Case, 310 F.3d 717, 741-42 (Foreign Intelligence Surveillance Ct. of Review 2002). Like the FISC, the Court of Review is established by FISA and provides a secret forum for the government to appeal decision by the FISC.

Judging by the volume of FISA requests, electronic surveillance for foreign intelligence purposes is a routine undertaking of the executive branch. Since its enactment in 1978, there have been more than 10,000 applications for FISA orders, and only one has been turned down.[85] The number of applications to the FISC has increased in recent years, topping 1,000 in the year 2000, a rate of nearly three applications per day.[86] Figures for FISA orders are only slightly lower than the rate of applications for Title III electronic surveillance warrants, which averaged approximately 1,100 per year between 1991 and 2001.[87]

D. Primary Purpose Test Survives FISA Which Leads to Department of Justice "Wall"

While FISA gave statutory approval to the foreign intelligence exception, the primary purpose test established in *United States v. Truong* limited its potential effect.[88] A number of courts confronted with questions regarding the admissibility of FISA surveillance held that the primary purpose test applied to evidence obtained under the new statute.[89] One such court observed, "[a]lthough evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance. The Act is not to be used as an end-run around the Fourth Amendment's prohibition of warrantless searches."[90]

The *Truong* court had held that the primary purpose of a surveillance operation could be determined by ascertaining the point at which law enforcement officers assumed control of the investigation from the intelligence officers who initiated it.[91] On the basis of this reasoning, the Justice Department decided that criminal prosecutors

85. NORMAN ABRAMS, ANTI-TERRORISM AND CRIMINAL ENFORCEMENT 419 (1st ed. 2003). Note that the figures for FISA orders include both new applications and requests for extension of existing orders.

86. *Id.* at 420.

87. *Id.*

88. The *Troung* court held that the Fourth Amendment required that any surveillance conducted pursuant to the foreign intelligence exception must be conducted for the primary purpose of collecting intelligence (as opposed to mounting a criminal investigation) in order for the fruits of the surveillance to be admissible at trial. 629 F.2d 908, 915 (4th Cir. 1980). *Truong* was decided after FISA became law, but the case arose prior to 1978; thus the statute was not at issue in the Fourth Circuit's decision.

89. *E.g.*, United States v. Duggan, 743 F.3d 59, 77 (2d Cir. 1984); United States v. Pelton, 835 F.2d 1067, 1076 (4th Cir. 1987).

90. United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991) (internal citations omitted).

91. *Truong*, 629 F.2d at 916.

could receive briefings on information gleaned from FISA surveillance but could not control its collection.[92] In practice, this arrangement proved workable until the 1994 espionage prosecution of Aldrich Ames.

The Ames investigation featured widespread exchanges of FISA-derived information between intelligence officers and the law enforcement personnel responsible for prosecuting the case.[93] After the case was resolved by plea bargain, Attorney General Janet Reno drafted new procedures to manage the flow of FISA material within the Justice Department.[94] The procedures were submitted to the FISC as the Department's new minimization procedures, as required by the FISA statute.[95] In approving the minimization procedures, the FISC predicted the regulations would promote "broad information sharing and coordination [between the intelligence officers and] the Criminal Division."[96] Over time, however, the procedures resulted in far less information sharing than had occurred previously because the Justice Department's Office of Intelligence Policy and Review ("OIPR") became the sole gatekeeper of FISA information.[97] The information flow withered so badly that the Department's FISA procedures became known simply as "the Wall."[98]

The procedures set forth by Attorney General Reno in 1995, and subsequently adopted by the FISC, aimed to preserve the admissibility of surveillance information obtained in the course of FISA investigations that uncovered evidence of criminal activity.[99] To that end, the FBI was charged with notifying prosecutors in the Justice Department's Criminal Division of any criminal information uncovered in the course of a foreign intelligence operation.[100] Once notified, prosecutors could offer "guidance" to the FBI, but were not to "instruct the FBI on the operation, continuation or expansion of FISA

92. NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 78 (2004) [hereinafter 9/11 COMMISSION REPORT].

93. *Id.*

94. *See generally* Reno memorandum, *supra* note 11.

95. *In re* All Matters Suhmitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 619 (Foreign Intelligence Surveillance Ct. 2002). Minimization procedures seek to prevent the unauthorized disclosure of FISA derived information by limiting the acquisition and retention of such information. 50 U.S.C. § 1801(h) (2004). The Justice Department's minimization procedures are required to be approved by the FISC. 50 U.S.C. §§ 1804(a)(5), 1823(a)(5) (2004).

96. *In re All Matters*, 218 F. Supp. 2d at 619.

97. 9/11 COMMISSION REPORT, *supra* note 92, at 79.

98. *Id.*

98. *See In re* Sealed Case, 310 F.3d 717, 727-28 (describing the 1995 procedures as an attempt "to avoid running afoul of the primary purpose test . . .").

100. Reno memorandum, *supra* note 11, at A6.

electronic surveillance or physical searches."[101] Communication between the two groups was to be coordinated by OIPR[102] to ensure that prosecutors did not assume control of the investigation.[103] The procedures also required OIPR to inform the FISC of any contacts between the FBI and the Criminal Division.[104] In cases where there were joint foreign intelligence and criminal investigations, the FISC would condition FISA renewals on the establishment of "Wall" procedures, which prevented criminal investigators from reviewing raw FISA material, "lest they become de facto partners in the FISA surveillances and searches."[105]

In practice, such "Wall" procedures proved very difficult to maintain and resulted in conflict between the FBI and the FISC over inappropriate sharing of FISA information.[106] In early 2000, the Justice Department formally notified the FISC of the unauthorized dissemination of FISA material in four or five cases.[107] Later that year, the Justice Department admitted that there were additional mistakes contained in 75 FISA applications related to investigations of potential terrorist attacks against the United States.[108]

In other instances, the "Wall" procedures were interpreted by the FBI as instituting impenetrable barriers between agents working on intelligence investigations and their colleagues working on criminal matters.[109] Pressure from the Justice Department and the FISC to ensure rigid FISA compliance eventually led to "walls" being erected between agents serving on the same squads.[110] The 9/11 Commission cited these breakdowns in communication as a significant barrier to the dissemination of intelligence regarding potential terrorist attacks against the United States in the years preceding the attacks on New York, Washington, and Pennsylvania.[111]

---

101. *Id.*

102. *Id.* at A1-A5.

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

104. Reno memorandum, *supra* note 11, at A7.

105. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620 (Foreign Intelligence Surveillance Ct. 2002).

106. 9/11 COMMISSION REPORT, *supra* note 92, at 79.

107. *In re All Matters*, 218 F. Supp. 2d at 620.

108. *Id.*

109. 9/11 COMMISSION REPORT, *supra* note 92, at 79.

110. *Id.*

111. *Id. See also In re* Sealed Case, 310 F.3d 717, 744 (Foreign Intelligence Surveillance Ct. of Review 2002) ("FISA court requirements based on *Truong* may well have contributed, whether correctly understood or not, to the FBI missing opportunities to anticipate the September 11, 2001 attacks.").

The uneven application of the "Wall" procedures was an inevitable outgrowth of the false dichotomy between the pursuit of foreign intelligence, on one hand, and investigations into criminal wrongdoing, on the other.[112] The notion that the two types of inquiries could be kept distinct, first promulgated by the Fourth Circuit in *Truong*, ultimately led the FISC to become involved in the internal workings of the FBI and the Justice Department.[113] This type of judicial intervention severely restricted the executive branch's ability to foster cooperation among all of its counter-intelligence personnel, including those pursuing criminal investigations.[114]

E. 9/11 prompts Congress to amend FISA

Although many people within the Justice Department and FBI had grown frustrated with the state of FISA procedures during the late 1990s,[115] changes to FISA did not become a political reality until after the 9/11 terrorist attacks. The attacks exposed how intelligence coordination failures contributed to the country's vulnerability.[116] Congress intended the changes promulgated in the Patriot Act to enhance FBI and Justice Department collaboration in cases where foreign intelligence and law enforcement purposes intersected.[117]

Section 218 of the Patriot Act amends § 1804(a)(7)(B) of FISA, changing the "purpose" standard for all new FISA applications.[118] Under the old FISA, federal officials who applied for FISA orders had to certify that the *purpose* of the proposed surveillance was the collection of foreign intelligence.[119] The Patriot Act lowered the bar by allowing officials to obtain a FISA order by showing that the collection of foreign intelligence is a *significant purpose* of the investigation.[120] The final wording of § 218 was the result of a compromise between the

112. *See id.* at 743 ("[C]riminal prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts.").

113. *Id.*

114. *Id.*

115. *See* Lerner, *supra* note 3, at 504 (discussing a pre-9/11 Justice Department lobbying effort to amend FISA to allow for more robust information sharing between intelligence officers and Criminal Division investigators); *see also* 9/11 COMMISSION REPORT, *supra* note 92, at 79 ("Separate reviews in 1999, 2000, and 2001 concluded independently that information sharing was not occurring.").

116. *See generally* Patriot Act, *supra* note 1.

117. Lerner, *supra* note 3, at 504.

118. Patriot Act, *supra* note 1, § 218.

118. *Id.*

120. *Id.* (emphasis added).

more sweeping amendment sought by the Justice Department and the status quo favored by civil libertarians.[121] The new significant purpose standard, which is not defined in the Patriot Act, was intended to improve the access of law enforcement officials to FISA information but prevent criminal prosecution from becoming the primary purpose of FISA surveillance.[122]

The Patriot Act also included several provisions intended to improve the exchange of FISA-derived information between intelligence and law enforcement officials. For example, Section 504 of the Act explicitly allows intelligence officers who conduct electronic surveillance to consult with law enforcement personnel to protect against "actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power."[123] In all of its changes, the Patriot Act made clear Congress's intent to allow more liberal use of FISA procedures, but the courts were left the task of determining just how liberal its application should be.

III. BEYOND CONGRESS'S WILDEST DREAMS: FISA COURT OF REVIEW RE-INTERPRETS 1978 ACT

A. A Secret Court Finds that the Patriot Act Does Not Go Far Enough

In the first published opinion in its history, *In re Sealed Case*, the FISA Court of Review overturned twenty-five years of FISA case law.[124] The court interpreted the pre-Patriot Act version of the statute to allow the use of FISA procedures to collect evidence of "foreign intelligence crimes."[125] In light of the FISA amendments contained in the Patriot Act, the Court of Review concluded that the "significant purpose" language enabled federal agents to collect FISA material for the purpose of prosecuting criminal activity as long as a foreign intelligence angle was also present.[126] Therefore, "[i]f . . . the application's purpose articulates a broader objective than criminal prosecution – such as stopping an ongoing conspiracy – and includes

121. *See* Lerner, *supra* note 3, at 504-05 (noting that the Justice Department proposed amending FISA's purpose standard to grant FISA orders where the collection of foreign intelligence was "a purpose" of the proposed surveillance).

122. *Id.* at 505.

123. Patriot Act, *supra* note 1, § 504(a).

123. *In re* Sealed Case, 310 F.3d 717, 746 (Foreign Intelligence Surveillance Ct. of Review 2002).

125. *Id.* at 724.

126. *See Id.* at 734-35 (interpreting FISA to allow surveillance "even if 'foreign intelligence' is only a significant—not a primary—purpose").

other potential non-prosecutorial responses, the government meets the statutory test."[127]

The FISA Court of Review was not content with the FISA standard set forth in the Patriot Act; accordingly, it set its sights on the primary purpose doctrine. It traced the evolution of the primary purpose doctrine to *Truong* and held that this limitation on the use of information obtained outside normal Title III warrant requirements did not survive after the passage of FISA.[128] The primary purpose test was not constitutionally required, according to the Court of Review, because it rested on a "false dichotomy" of foreign intelligence information versus law enforcement evidence.[129] The collection of foreign intelligence and the investigation of criminal activity rested on the unstated assumption that "the government seeks foreign intelligence . . . for its own sake – to expand its pool of knowledge – because there is no discussion [in any of the FISA cases] of how the government would use that information outside criminal prosecutions."[130] In overturning the primary purpose doctrine, the Court of Review, sitting *ex parte*, implicitly overruled the Fourth Amendment holdings of numerous FISA cases.[131]

The Court of Review's Fourth Amendment analysis in *In re Sealed Case* rested on a lengthy comparison of the requirements for Title III electronic surveillance warrants and FISA orders.[132] The analysis addressed the three elements of the Fourth Amendment's warrant clause: (1) the approval of a neutral magistrate, (2) the requirement that the warrant's proponent demonstrate probable cause that "the evidence sought will aid in a particular apprehension or conviction" and, (3) the requirement that the target of the warrant be described particularly.[133] The court found substantial similarity between Title III and FISA for the first element: both statutes require the approval of a judge before a warrant for electronic surveillance can be issued,[134] and even though it operates in secret, the FISC is considered a "detached and neutral body."[135]

---

127. *Id.* at 735.

128. *Id.* at 724-26.

129. *Id.*

130. *Id.* at 727.

131. *E.g.*, United States v. Duggan, 743 F.3d 59 (2d Cir. 1984); United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987); United States v. Badia, 827 F.2d 1458 (11th Cir. 1987).

132. *In re Sealed Case*, 310 F.3d at 737.

133. *Id.* at 738 (citing Dalia v. United States, 441 U.S. 238, 255 (1979)).

134. 50 U.S.C. § 1805 (2004); 18 U.S.C. § 2518 (2004).

135. United States v. Cavanagh, 807 F.2d 787, 790 (9th Cir. 1987).

Addressing the second element, the court found that although both Title III and FISA require the proponent of a warrant or order for electronic surveillance to demonstrate probable cause, the required showings differ.[136] Title III requires the proponent to demonstrate probable cause that the target is about to commit or has committed one of the crimes enumerated by the statute.[137] FISA, on the other hand, requires probable cause that the target is "a foreign power or agent of a foreign power."[138] Elsewhere in the statute, the definition of "agent of a foreign power" includes a reference to criminal activity, but under a standard much lower than probable cause.[139] This lower standard of evidence reflects a congressional judgment that foreign intelligence crimes are more difficult to detect.[140] The Court of Review reasoned that this lower standard is offset by the FISA requirement of probable cause to believe that the target is working for a foreign power.[141]

FISA and Title III also differ significantly with regard to the Fourth Amendment requirement that a target of surveillance be described with particularity. FISA's only nod to this requirement is that FISA orders are only available for the collection of foreign intelligence.[142] Title III, on the other hand, requires probable cause that communications indicative of a specified crime will be obtained,[143] but does not require the proponent to identify any information about the individual targeted by the surveillance.[144] Based on what it perceived as the relative balance in protections afforded under Title III and FISA, the Court of Review concluded that "to the extent a FISA order comes close to meeting Title III . . . [this] certainly bears on its reasonableness under the Fourth Amendment."[145]

---

136. 18 U.S.C. § 2518(3)(a) (2004); 50 U.S.C. § 1805(a)(3) (2004).

137. 18 U.S.C. § 2518(3)(a) (2004).

138. The probable cause showing is subject to the limitation that a citizen or permanent resident of the United States may not "be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States." 50 U.S.C. § 1805(a)(3)(A) (2004).

139. An agent is anyone 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 United States." 50 U.S.C. § 1801(b)(2)(A) (2004) (emphasis added).

140. *In re* Sealed Case, 310 F.3d 717, 739 (Foreign Intelligence Surveillance Ct. of Review 2002).

141. *Id.*

142. *Id.* at 740.

143. 18 U.S.C. § 2518(3)(b) (2004).

144. *In re Sealed Case*, 310 F.3d at 740 (citing United States v. Kahn, 415 U.S. 143, 157 (1974)).

145. *Id.* at 742.

The broad FISA powers recognized by the Court of Review were welcomed by federal prosecutors.[146] Attorney General Ashcroft made available "millions of pages of existing FISA evidence" to federal prosecutors and claimed that the court victory would "revolutionize our ability to investigate terrorists."[147] Despite predictions that the exposure of intelligence sources and methods would discourage such disclosures,[148] FISA-derived evidence has begun surfacing in prosecutions across the country.[149]

B. The New FISA: A Much Needed Improvement or Ripe for Over-Reaching?

In its decision overhauling the FISA landscape, the Court of Review stressed that the primary purpose test had frustrated the purpose of the FISA by unduly restricting the executive branch's ability to protect the country from foreign threats.[150] The line that had been initially drawn by the *Truong* court between acceptable and unacceptable purposes "rested on a false premise" that as the government proceeds with a criminal prosecution, its foreign intelligence "purpose" wanes.[151] The various statutory references to criminal activity, according to the Court of Review, make clear that Congress "did *not* preclude or limit the government's use . . . of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution."[152] For instance, FISA's definition of foreign intelligence information includes evidence of crimes such as espionage, sabotage, or terrorism.[153] Furthermore, the statutory definition of "an agent of a foreign power" is in part based on the presence of criminal conduct.[154]

---

146. *See* Glenn R. Simpson & Jess Bravin, *Prosecutors Capitalize on Increased Access to Wiretap Evidence*, WALL ST. J., Jan. 21, 2003, at A4 ("Law enforcement authorities say such [FISA] information – previously unavailable for criminal prosecutions – is breathing new life into numerous antiterrorism cases or significantly strengthening them.").

147. *Id.*

148. *Id.*

149. *See id.* (describing the use of FISA information in prosecutions in New York, Illinois, Florida, and Texas); *see also* David Rosenweig & Greg Krikorian, *Ex-Agent Indicted in Spying Probe*, L.A. TIMES, December 11, 2004, at B1 (identifying a case in which FISA-authorized evidence was admitted into evidence); Mark Hamblett, *Stewart Jury Watches First Tapes of Meeting with Client in Prison*, N.Y. L.J., August 15, 2004, at 1 (same).

150. *In re Sealed Case*, 310 F.3d at 744-45.

151. *Id.* at 743.

152. *Id.* at 727 (emphasis in original).

153. *Id.* at 723.

154. *Id.*

The Court of Review also criticized the "Wall" procedures adopted by the FISC for perhaps contributing to the vulnerability of the United States.[155] "Effective counter-intelligence," the Court of Review explained, "requires the wholehearted cooperation of all the government's personnel who can be brought to the task."[156] The 9/11 Commission went one step further, explicitly linking the dearth of information sharing that resulted from the "Wall" procedures to the government's ignorance of the 9/11 plot.[157]

Professor Craig Lerner contends that the Court of Review's decision appropriately returns the question of the balance between national security and privacy rights to Congress and the executive.[158] For support, Lerner points out that over time, this balance had been distorted by the misguided implementation of the "Wall" procedures, particularly in the day-to-day management role performed by the FISC.[159] This tug-of-war between the secret court and the executive branch obscured the widely recognized executive power to carry out warrantless surveillance in the pursuit of foreign intelligence information.[160] The resolution of conflicts between this inherent power and the consequent compromises to privacy rights is a "political question," according to Professor Lerner, and should not be resolved "in a secret chamber of unelected judges themselves appointed by an unelected judge."[161]

Critics of the Patriot Act amendments to FISA and the subsequent decision by the FISA Court of Review argue that resultant improvements in intelligence coordination do not justify the potential that FISA will be employed as an end-run around the Fourth Amendment.[162] Instead of foisting the balance between privacy and national security on the elected branches, civil libertarians assert:

---

155. *See id.* at 744 (discussing congressional testimony suggesting that "the FISA court requirements based on *Truong* may well have contributed, whether correctly understood or not, to the FBI missing opportunities to anticipate the September 11, 2001 attacks").

156. *Id.* at 743.

157. 9/11 COMMISSION REPORT, *supra* note 92, at 78-79.

158. Lerner, *supra* note 3, at 512.

159. *See id.* at 510 ("The patent inability of the FBI and DOJ to maintain walls separating inextricably intertwined investigations might have alerted the FISA [court] to the wrongheadedness of the prevailing interpretation. Instead, the FISA court hewed ever more fixedly, and quixotically, to an interpretation that was revealed as unworkable.").

160. *Id.* at 511.

161. *Id.*

162. *See, e.g.*, Rackow, *supra* note 36, at 1675; Jennifer C. Evans, *Hijacking Civil Liberties: The USA Patriot Act of 2001*, 33 LOY. U. CHI. L.J. 933, 974-75 (2002) ("The wiretapping and intelligence provisions in the USA PATRIOT Act improperly minimize the role of judges in ensuring that law enforcement wiretapping is conducted legally and permits intelligence authorities to bypass procedures that protect people's privacy.").

"When the overriding purpose of a surveillance request is unclear, preserving the privacy interests of a potentially innocent target should be a higher priority than facilitating the receipt of surveillance authority."[163]

The Fourth Amendment entrusts the protection of individuals from invasions of privacy by law enforcement officials to the judiciary. Recasting this question as political ignores the history of executive overreaching in the name of foreign intelligence collection. The expansion of executive power under the amended FISA regime sets in motion a conflict that the Constitution demands be settled with due regard for privacy interests.[164] On the other hand, returning to the pre-9/11 status quo cannot be considered a practical option in light of the highly critical findings of the 9/11 Commission.

C. The Court Is Correct on One Count: The Pre-9/11 System was Broken and Requires Fixing

In its drive to rigidly adhere to the "Wall" procedures, the Justice Department (with help from the FISC) created an enforcement regime so complex and cumbersome that its own personnel were often unable to comply with it.[165] Unfortunately, the problems related to information sharing were not exposed until the 9/11 investigations clearly demonstrated the lack of coordination that plagued the intelligence community.[166] In 2000 alone, the Justice Department confessed to the FISC more than 80 instances in which its officials had not complied with the minimization procedures it promulgated in the wake of the Aldrich Ames investigation.[167]

Even when the FISA process was a viable route, the time involved in obtaining the necessary bureaucratic approvals often rendered the information obsolete.[168] The bureaucratic inertia surrounding FISA information became so dire that, in some cases, FBI agents assigned to FISA investigations were not sharing information

---

163. Rackow, *supra* note 36, at 1680.

164. *See* Berger v. New York, 388 U.S. 41, 63 (1967) ("Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices.").

165. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620-21 (Foreign Intelligence Surveillance Ct. 2002).

166. *See generally* 9/11 COMMISSION REPORT, *supra* note 92.

167. *Id.*

168. *See* Lerner, *supra* note 3, at 503 (explaining that even if FBI headquarters would have approved a FISA request from its Minneapolis field office to search the laptop computer of Zacarias Moussaoui, the alleged 20th hijacker of 9/11, the internal FISA approval process would not have been completed by September 11).

with agents on their squad who were attempting to build a criminal case.[169] The misunderstandings surrounding FISA also gave rise to the misguided belief within the FBI that intelligence information, regardless of its source, could not be shared with agents working on criminal investigations.[170] As a result, relevant information the FBI had received from intelligence agencies, such as the CIA and NSA, was withheld from criminal investigators.[171]

Given this backdrop of bureaucratic infighting and lack of coordination, the need to streamline FISA procedures in the wake of 9/11 is apparent. Through the amendments included in the Patriot Act, Congress emphasized the need for FISA orders to be more readily attainable[172] and for the information obtained pursuant to FISA orders to be shared more liberally within the government.[173] These changes, while significant, did not fundamentally alter the existing line between intelligence collection and law enforcement that served as the baseline for the Wall procedures. Not content to merely interpret the Patriot Act amendments, the Court of Review overturned twenty years of Fourth Amendment case law relative to FISA in an *ex parte* proceeding. Two amicus briefs provided the only opposing voices considered by the court.[174]

D. FISA Court of Review Decision Overreaches

In its overhaul of FISA procedures, the Court of Review correctly recognized that the interpretation of the primary purpose test embodied in the "Wall" procedures resulted in a wholly unsatisfactory and often ineffective enforcement process.[175] The stagnant flow of information, and its effects on the government's

169. 9/11 COMMISSION REPORT, *supra* note 92, at 79.

170. *Id.*

171. *Id.*

172. *See* Patriot Act, *supra* note 1, § 218 (amending the FISA requirement that the collection of foreign intelligence information be the "purpose" of a surveillance order to the lower standard that the collection of such information be "a significant purpose" of the surveillance).

173. *See id.* at § 504(a) (providing for consultation between federal officers who collect foreign intelligence information and law enforcement officials when certain conditions are met; *id. at* § 905 (requiring the Justice Department to share foreign intelligence information acquired in the course of a criminal investigation with the Director of Central Intelligence).

174. *See In re* Sealed Case, 310 F.3d 717, 719 (Foreign Intelligence Surveillance Ct. of Review 2002) ("Since the government is the only party to FISA proceedings, we have accepted briefs filed by the American Civil Liberties Unions and the National Association of Criminal Defense Lawyers as *amici curiae*.").

175. *See id.* at 743 ("A standard which punishes . . . cooperation could well be thought dangerous to national security.").

ability to protect the nation, has been explored in detail by independent investigations before and after the 9/11 attacks.[176]

The Court of Review appropriately criticized the FISC for not affording sufficient deference to the Patriot Act amendments in an earlier decision: "We . . . think the refusal by the FISA court to consider the legal significance of the Patriot Act's crucial amendments was error."[177] However, instead of outlining the effect of the Patriot Act amendments, the Court of Review turned back the clock more than twenty years to attack the primary purpose test.[178] In doing so, the court expressly acknowledged that rescinding the division between intelligence collection and law enforcement rendered the intent behind the Patriot Act amendments paradoxical because the Act recognized just such a dichotomy.[179] That conundrum was resolved by a rather creative episode of statutory interpretation, which concluded that the debate over the significance of the division was largely academic. The court noted that "typically [the government] will not have decided whether to prosecute the agent [who is the target of FISA surveillance]. So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test."[180]

This new significant purpose test, while arguably easy to meet in any investigation involving foreign intelligence, is defensible in light of the Patriot Act amendments. The Court of Review overreached, however, in holding that the determination of the significance of the foreign intelligence purpose should be left to the executive branch official who certifies the FISA application.[181] Thus, in reviewing FISA applications, the FISC is prohibited from making any factual inquiry into the status or staffing of the Justice Department investigation in an effort to examine the true purpose motivating the request for a FISA order.[182] This concentration of

176. 9/11 COMMISSION REPORT, *supra* note 92, at 78-79; *see also In re Sealed Case*, 310 F.3d at 727 (citing pre-9/11 reports by the General Accounting Office and a team appointed by the Attorney General to review the Los Alamos National Laboratory Investigation and noting that both reports criticize the lack of coordination between intelligence officers and law enforcement officials that resulted from rigid enforcement of the 1995 procedures).

177. *In re Sealed Case*, 310 F.3d at 732.

178. *See id.* at 742-45 (characterizing the analysis in *Troung* as resting "on a false premise" and deriding the primary purpose test as "inherently unstable, unrealistic, and confusing").

179. *See id.* at 734-35 ("[P]aradoxically, the Patriot Act would seem to conflict with the government's first argument because by using the term 'significant purpose,' the Act now implies that another purpose is to be distinguished from a foreign intelligence purpose.").

180. *Id.* at 735.

181. *Id.* at 736.

182. *Id.*

decisionmaking authority in the executive branch relative to a much weaker "significant purpose" standard removes the possibility of any meaningful judicial oversight of executive actions pursuant to the foreign intelligence exception to the warrant requirement.

The Court of Review's equation of requirements for obtaining a FISA order and a Title III surveillance warrant also deserves closer examination. The probable cause requirements for the two determinations differ significantly: Title III requires probable cause to believe a crime has been or is about to be committed, whereas FISA mandates probable cause that the target of surveillance is an agent of a foreign power.[183] The designation of "agent of a foreign power" can be made for any of a number of reasons, but there is no requirement that the application present any reason to believe that a crime has occurred or is imminent.[184] Thus, under FISA, a surveillance application can be approved where the target's actions "may involve" criminal activity,[185] a considerably lower standard than the Title III probable cause requirement. Allowing government surveillance under such a low showing in every conceivable FISA case is incompatible with the Fourth Amendment's probable cause requirement.[186]

The notion that the Court of Review appropriately returned the question of how to balance national security and the privacy rights of individuals to the elected branches is reminiscent of earlier times in U.S. history when the executive branch routinely cited its national security power as license to initiate wide ranging surveillance operations.[187] FISA established limits on a previously unchecked executive power and empowered the judiciary to oversee compliance with the statutory scheme indicating that Congress sought to rein in national security surveillance.[188] If a reconsideration of the balance between national security and privacy is warranted, Congress should initiate this through legislation (as it did in the Patriot Act) and the judiciary should review and interpret this legislation through the

183. *See supra* text accompanying note 74.

184. 50 U.S.C. § 1801(b)(2)(a) (2004).

185. *Id.*

186. *See supra* text accompanying note 133 (enumerating elements of a Fourth Amendment search warrant); *see also* Grayson A. Hoffman, Note, *Litigating Terrorism: The New FISA Regime, the Wall, and the Fourth Amendment*, 40 AM. CRIM. L. REV. 1655, 1672-74 (2003) (providing a detailed critique of the Court of Review's probable cause analysis).

187. *See generally* Banks & Bowman, *supra* note 17 (detailing the history of Executive surveillance pursuant to its national security powers).

188. *See* ABRAMS, *supra* note 85, at 418 ("Viewed against this historical backdrop, rather than expanding federal authority, FISA can be seen as a statute that reined in the Executive Branch, regulating a kind of electronic eavesdropping that previously had been uncontrolled by the judiciary.").

normal adversarial process. Review by a secret court, where constitutionally guaranteed interests are represented only by amicus briefs, does not give full airing to the privacy concerns implicated by the Patriot Act's FISA amendments.

IV. SOLUTION: STRICT ENFORCEMENT OF SIGNIFICANT PURPOSE IN CRIMINAL PROSECUTIONS

Where a prosecutor seeks to introduce evidence obtained through FISA in a criminal proceeding, Fourth Amendment concerns will inevitably arise. Thus, the analysis of the constitutional framework for the "new" FISA revolves primarily around the role of foreign intelligence information in the criminal process. This Section, therefore, is limited to the question of when FISA-derived information can constitutionally be introduced against a criminal defendant.[189] It also provides a comprehensive proposal for how the amended FISA, including the provisions related to intelligence coordination, should operate in practice.

A. Returning to the Truong Functional Analysis

In its pre-FISA analysis, the *Truong* court drew on the relative competencies of the executive and judiciary in outlining the scope of the foreign intelligence exception. If it is indeed true that FISA embodied Congress's attempt to rein in the executive intelligence-gathering power,[190] the *Troung* analysis is an appropriate starting point for determining the constitutional scope of the post-Patriot Act FISA.[191]

Since regular Article III courts "possess expertise in making the probable cause determination involved in surveillance of suspected criminals,"[192] judicial review under Title III should be utilized to review all search applications where the government seeks to initiate electronic surveillance in criminal investigations. When the

189. For the sake of clarity, the analysis will be limited to the introduction of FISA-derived evidence against United States citizens.

190. ABRAMS, *supra* note 85, at 418.

191. The FISA Court of Review took a different approach, casting aspersions on *Troung* (e.g., "[w]e reiterate that *Troung* dealt with a pre-FISA surveillance . . ."), and ignoring its functional analysis altogether. Instead, the court took aim at the notion that foreign intelligence concerns and law enforcement interests were mutually exclusive and concluded that FISA amplified the Executive power by creating a process that "approaches a classic warrant and [is] therefore . . . constitutionally reasonable." *In re* Sealed Case, 310 F.3d 717, 742-45. (Foreign Intelligence Surveillance Ct. of Review 2002).

192. United States v. Truong, 629 F.2d 908, 913 (4th Cir. 1980).

government investigates a crime, whether it be espionage or armed robbery, that it suspects has already occurred, for instance, courts are well-suited to make probable cause determinations.

The courts are, however, "unschooled in diplomacy" and thus not functionally equipped to "judge the importance of particular information to the security of the United States."[193] As the FISA Court of Review explained, the government's law enforcement concern in procuring intelligence information is to stop or frustrate the immediate criminal activity: "Punishment of the terrorist or espionage agent is really a secondary objective; indeed, punishment of a terrorist is often a moot point."[194] The FISA process should therefore be reserved for instances in which the executive branch targets ongoing foreign threats. The primary objective is neutralizing the threat; any prosecution that results is clearly a secondary effect.

A functional approach to the authorization of electronic surveillance would restore the balance between FISA, Title III, and the Fourth Amendment. Under the limited circumstances where the executive branch gathers foreign intelligence information that is later relevant in a criminal proceeding, deference to the FISA process is reasonable.[195] In all other investigative contexts, the Fourth Amendment mandates that the privacy interests of individuals are a foremost concern. Title III is thus the appropriate process for authorizing electronic surveillance because it was designed to protect the Fourth Amendment concerns inherent in such intrusive observation.

B. Rethinking the Role of the FISC

In order to accomplish the dual objectives of improving intelligence coordination and complying with the Fourth Amendment, analysis of the constitutionality of FISA information should be conducted in the mainline Article III courts where prosecutors seek to introduce FISA-derived evidence. This judicial review would occur in the context of motions to exclude evidence in criminal trials. The new FISA, furthermore, should not impede intelligence-sharing within the executive branch. Any breakdown in intelligence coordination, similar to what occurred in the aftermath of the "Wall" procedures, would

193. *Id.* at 913-14.

194. *In re Sealed Case*, 310 F.3d at 744-45.

195. This view is slightly different than the primary purpose formulation that originated in *Truong*, because as the Court of Review pointed out, investigating an ongoing instance of a foreign intelligence crime such as espionage, while primarily a criminal investigation, demands the flexibility that FISA provides.

handicap the government's ability to defend against large-scale terrorist attacks.

The desired balance between the government's intelligence collection powers and the Fourth Amendment rights of an accused is difficult to achieve. Once FISA-derived evidence is presumed admissible in criminal trials, it is difficult to restrict the evidence's use to certain types of criminal investigations. Without restrictions, however, FISA becomes a tempting avenue for criminal investigators to gather information when they are unable to (or prefer not to) meet Title III's more demanding standards. This determination is particularly problematic under the amended FISA because the Patriot Act provides no indication of what constitutes the significant foreign intelligence purpose necessary to obtain a FISA surveillance order.[196]

The FISC is ill-equipped to determine the constitutionality of each FISA application. It is not functionally prepared to balance the Fourth Amendment concerns inherent in the nearly 1,000 applications for surveillance it receives each year. The FISC was established to afford significant deference to the executive in the field of foreign intelligence collection[197] because mainline Article III courts were not considered competent "to judge the importance of particular information to the security of the United States."[198] Since its creation, this secret court has demonstrated that it is no better equipped to balance intelligence needs against the rights of subsequent defendants than district courts. The FISC's attempts to distinguish between foreign intelligence investigations and criminal investigations by analyzing which part of the Justice Department was involved in a particular case were quite possibly unconstitutional[199] and ultimately resulted in the flow of FISA information withering to a virtual halt.[200]

Instead of conducting a searching review of each FISA application, the FISC should limit its review to ensuring that each request facially meets the statutory criteria (*e.g.*, significant foreign intelligence purpose, probable cause to believe that the target is an agent of a foreign power). It is not realistic to expect the court to serve

196. 50 U.S.C. § 1804(a)(7)(B) (2004). This statute was amended by the Patriot Act to require "that a significant purpose of the surveillance is to obtain foreign intelligence information." *Id.*

197. *See* United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984) ("The FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information.").

198. United States v. Truong, 629 F.2d 908, 914 (4th Cir. 1980).

199. *See In re* Sealed Case, 310 F.3d 717, 731 (Foreign Intelligence Surveillance Ct. of Review 2002) ("[T]he FISA court may well have exceeded the constitutional bounds that restrict an Article III court.").

200. 9/11 COMMISSION REPORT, *supra* note 92, at 79.

as an effective constitutional gatekeeper. By definition, the court relies on certifications provided by executive branch applicants and is relatively isolated from effective review.[201]

If the FISC review is limited to checking that the certifying officer has correctly completed the FISA application, district courts must recognize the expanded reach of FISA. Accordingly, they must conduct more searching Fourth Amendment reviews when a prosecutor seeks to admit FISA-derived evidence in a criminal proceeding. In the course of these reviews, evidence must only be admitted if the prosecution demonstrates that the FISA evidence was uncovered in the course of protecting the country from foreign powers.

C. Applying a New (and Improved) FISA Standard

Reviews of FISA-derived evidence by traditional Article III courts should be conducted under an abuse of discretion standard. This standard recognizes that the judiciary owes some degree of deference to the foreign intelligence decisions of the executive branch and the FISC. The review should also be flexible so that courts can consider those factors that are most indicative of the government's foreign intelligence purpose in a particular case. The information evaluated should include which subdivisions of the Justice Department were involved in the investigation. This type of consideration should not be confused with the judicial interference in the affairs of the Justice Department that the Court of Review suggested violated separation of powers principles. Instead, the consideration of which investigators were involved in the case should be a flexible inquiry that constitutes one of a number of factors a court considers in determining whether information was legitimately obtained under a FISA order. Other factors include the scope of the investigation that resulted in the prosecution, the nature of the pending charges, and whether the information sought pursuant to the FISA order was more appropriately the subject of a Title III request.

The new FISA standard will necessarily leave a significant amount of discretion to trial courts, but language from the FISA itself can help determine whether evidence was obtained in the course of a legitimate intelligence operation. For instance, the statutory definition of "foreign intelligence information" includes information related to a number of potential criminal activities such as sabotage,

201. *See* Rackow, *supra* note 36, at 1671 (noting that the FISC has denied only one request in its history and approved more than 1,000 orders in 2001 alone).

terrorist acts, and clandestine intelligence activities.[202] This new standard will, therefore, be different from the primary purpose test in that it will not require a bright line between criminal prosecution and collecting foreign intelligence information, the two of which sometimes intersect.[203] Thus, when the government prosecutes an individual for activity closely related to the type of criminal activity described by the statute, the admission of FISA-derived evidence should be admitted since no Fourth Amendment concerns are implicated.[204] For instance, there should be little controversy over the admissibility of FISA-derived evidence when the government seeks to introduce it in an espionage prosecution against a CIA officer.[205]

The government could also satisfy the new FISA standard by showing that, at the time the FISA order was obtained, there existed probable cause to conclude that the defendant was an agent of a foreign power as defined by the statute.[206] This standard could be easily met in a case like *Truong*, for instance, where the investigation involved espionage and there was probable cause to believe that the defendant was an agent of a foreign government.[207] Once again, the analysis here is cleaner and more faithful to the FISA than the primary purpose test; if the FISA order was supportable by probable cause linking the defendant to a foreign power, the abuse of discretion standard cannot be met.[208]

In opposing the admission of FISA-derived evidence, the defendant will be free to argue that the evidence presented against him was not obtained with a "significant purpose" of collecting foreign intelligence. If a trial court determines that the FISA order in

---

202. 50 U.S.C. § 1801(e)(1) (2004).

203. *See In re Sealed Case*, 310 F.3d at 727 ("The government's overriding concern is to stop or frustrate the . . . foreign power's activity by any means, but if one considers the actual ways in which the government would foil espionage or terrorism it becomes apparent that criminal prosecution analytically cannot be placed easily in a separate response category.").

204. Another option would be to amend FISA to allow automatically (or establish a rebuttal presumption in favor of) the admission of evidence obtained pursuant to the statute when it is introduced against a defendant charged with certain enumerated offenses, including foreign-based terrorism, espionage, etc.

205. *See* 9/11 COMMISSION REPORT, *supra* note 92, at 78 (describing Justice Department concerns that the primary purpose standard jeopardized tbe admissibility of a significant amount of FISA-derived evidence in the espionage prosecution of Aldrich Ames).

206. *See* 50 U.S.C. § 1805(a)(3)(A) (2004) (authorizing the issuance of a FISA order when there is probable cause to believe that the target of surveillance is an agent of a foreign power); 50 U.S.C. § 1801(b) (2004) (defining "agent of a foreign power").

207. *See generally* United States v. Truong, 629 F.2d 908 (4th Cir. 1980).

208. *See* Lerner, *supra* note 3, at 500 (describing the concern of many within the law enforcement and intelligence communities that much of the evidence against Aldrich Ames was susceptible to challenge because it was obtained pursuant to a FISA order while the investigation was being directed by law enforcement officials).

question lacked the requisite purpose and instead constituted an abuse of discretion, Fourth Amendment considerations compel the suppression of the evidence. Such a challenge might be successful if the crime being investigated was only tenuously connected to the foreign intelligence purpose specified in the FISA order. For instance, a FISA order to investigate drug trafficking by a street gang on the basis that one of the gang's leaders is a Muslim convert who periodically worships at a mosque that is suspected of ties to terrorism would be suspect. To admit evidence obtained as a result of the order, the prosecutor would have to show that a significant purpose of the investigation was to procure foreign intelligence information.[209] Based on the facts provided, a judge could find that the FISC abused its discretion in issuing the order.

Requiring district courts to conduct this expanded determination will require more scrutiny than previously required under FISA; however, the judiciary is well equipped to make this sort of Fourth Amendment determination. This expanded review will also improve upon the paradigm used by the Court of Review to balance the Fourth Amendment rights of the accused against the government interest in increased coordination of foreign intelligence collection. Under the regime proposed by the Court of Review, the scrutiny of government certifications would be cursory at both the FISC and the trial stage, thus risking the wholesale disregard of Fourth Amendment considerations in FISA cases.

V. CONCLUSION

Implementing any FISA regime entails delicately balancing the government's need for foreign intelligence with the Fourth Amendment interests of individuals targeted by federal surveillance. In order to effectuate the "significant purpose" language of the Patriot Act amendments to FISA, courts need flexibility in determining whether FISA-derived evidence is properly admitted at trial. An abuse of discretion standard that provides courts with a range of factors to analyze will allow courts to better decide cases where foreign intelligence issues are clearly in play. It will also give courts the guidance they need to make admissibility decisions in tougher cases under the existing statutory scheme.

209. 50 U.S.C. § 1804(a)(7)(B) (2004).

The need for a new FISA standard is clear in light of the existing alternatives. The primary purpose doctrine originated from a sound analysis of the relative competencies of the executive and the judiciary, but it evolved into a test in which the outcome depends entirely on which type of law enforcement agents were involved in an investigation at a specific point in time. In addition to being unwieldy, this intrusive inquiry contributed directly to the intelligence failures underlying the 9/11 attacks. Similarly handicapping the government now would risk another catastrophic intelligence failure in addition to ignoring the changes to FISA contained in the Patriot Act.

On the other hand, the FISA Court of Review's decision flipped the balance too far in the opposite direction. By implementing a standard that goes beyond any conceivable intent of the Patriot Act's drafters, the Court of Review has established a system where FISC review is cursory and trial court review is practically non-existent. The fact that a secret court sitting *ex parte* saw fit to pass judgment on the constitutionality of its expansive reading of FISA under the Fourth Amendment indicates, at a minimum, that the court's decision deserves very close scrutiny.

The well-documented abuses that occurred in the name of foreign intelligence-gathering in the pre-FISA period suggest that deference to the executive in such matters poses significant risks.[210] While the need to improve intelligence collection and coordination in the post-9/11 environment is undeniable, history counsels that courts should ease the restrictions on the executive branch only after careful consideration.[211]

210. *See* Rackow, *supra* note 36, at 1666 (describing how, before FISA, "the absence of clear statutory or judicial standards led to widespread warrantless electronic surveillance of individuals who were not associated in any way with a foreign power, did not seem to pose a threat to national security, and were not suspected of being involved in criminal activity").

211. *See id.* at 1694-95 (cautioning that the invocation of the needs of government during wartime to increase intelligence collection has led to significant deprivations of civil rights).

A functional balance between FISA and the Fourth Amendment can only be struck when traditional Article III courts analyze the intersection of these competing concerns in various factual contexts. As it stands now, however, courts must continue to grant significant deference to the executive branch in the foreign intelligence context, while also establishing a mechanism to stop the executive branch from pursuing its intelligence goals into unconstitutional areas. The proposed Article III review process would ensure that these competing interests are balanced appropriately.

J. Christopher Champion[*]

* Candidate, Doctor of Jurisprudence, Vanderbilt University Law School, May 2006.
Thanks to everyone involved with the law review for their role in making this Note a reality. Particular thanks to Russ Taher, Rob Peal, and Amanda Ambrose for their insights into improving the substance and structure of my tboughts. Thanks also to my wife, Ana, for her understanding and support throughout my law school adventure.

***