Cutting the Fourth Amendment Loose from Its Moorings: The Unconstitutional Use of FISA Evidence in Ordinary Criminal Prosecutions

by KATHLYN QUERUBIN*

> Our Government is the potent, the omnipresent teacher. For good or ill, it teaches the whole people by its example.... [I]f the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy.... [T]o declare that the Government may commit crimes in order to secure the conviction of a private criminal—would bring terrible retribution. Against that pernicious doctrine this Court should resolutely set its face.
>
> *–Justice Louis D. Brandeis*[1]

Introduction

Immediately after the terrorist attacks of September 11, 2001, several journalists and senators claimed that intelligence agencies failed to "connect the dots" and thwart the attacks.[2] Although law enforcement and intelligence agencies had information on some of the hijackers and the possibility of using planes as weapons prior to September 11, critics charged that these agencies failed to share and

---

* J.D. Candidate 2010, University of California, Hastings College of the Law; B.A. *magna cum laude*, 2003, Politics and History, University of San Francisco. The author wishes to thank the editorial staff at the *Hastings Constitutional Law Quarterly* for their hard work; Professor Peter Keane for his inspiration and guidance, Barry and Janet Portman for their expert counsel, and Jose and Rosario Querubin for their tremendous support. The author also extends special thanks to Daniel Portman, whose unwavering encouragement made this Note and many other things possible.

1. Olmstead v. United States, 277 U.S. 438, 485 (1928) (Brandeis, J., dissenting).

2. *See* Richard Cohen, *The Terrorism Story—And How We Blew It*, WASH. POST, Oct. 4, 2001, at A31; Evan Thomas & Mark Hosenballs, *How He'll Haunt Us*, NEWSWEEK, Dec. 31, 2001, at 14.

coordinate information among themselves in a way that could have prevented the tragedy that followed.[3] Congress responded to these charges with unprecedented speed. On October 2, 2001, only a few weeks after the attacks, Representative F. James Sensenbrenner, Jr. (R-Wisc.) introduced a bill that purported to improve cooperation between law enforcement and intelligence communities to combat terrorism.[4] The bill would later become known as the USA PATRIOT ACT ("Patriot Act").[5]

The Patriot Act amended several existing statutes including the Foreign Intelligence Surveillance Act of 1978 ("FISA").[6] FISA had been originally enacted to impose Fourth Amendment protective procedures on the government's power to conduct electronic surveillance for the purpose of gathering foreign intelligence.[7] In order to get judicial authorization to conduct electronic surveillance, FISA required the investigatory agents to demonstrate to a special Foreign Intelligence Surveillance Court ("FISC") judge that "the purpose" of their intended surveillance was the collection of foreign intelligence information, as opposed to ordinary law enforcement.[8] Courts have interpreted this provision to require the government to demonstrate that foreign intelligence was the "*primary* purpose" of the FISA investigation.[9] Thus, FISA ensured that traditional criminal

3. David Rogers & David Cloud, *Poor Cooperation May Have Delayed Moussaoui Search*, WALL ST. J., May 21, 2002, at A8.

4. Edel Hughes, *Entrenched Emergencies and the "War on Terror": Time to Reform the Derogation Procedure in International Law?*, 20 N.Y. INT'L L. REV. 1, 50-51 (2007).

5. 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] (codified in scattered sections of 8, 12, 18, 21, 22, 28, 31, 47, and 50 U.S.C.).

6. Originally enacted as the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, §§ 103, 104(a)(7)(A)–(C), 92 Stat. 1783, 1788–89 (1978) [hereinafter FISA] (codified as amended at 50 U.S.C. §§ 1801–1863 (2006)). Although FISA authorizes the Executive to conduct physical searches, as well as electronic surveillance with judicial authorization from a special Foreign Intelligence Surveillance Court, this Note only examines the portions of FISA that regulate electronic surveillance in the United States.

7. William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1214–15 (2007) (lamenting that the central premise of FISA—"authorizing secret electronic surveillance for the purpose of collecting foreign intelligence, but subjecting applications to judicial scrutiny and the entire process to congressional oversight"—was lost after it was amended by the Patriot Act).

8. *See* FISA, *supra* note 6. The amended version of FISA only requires that the government demonstrate that "the target of the electronic surveillance is a foreign power or an agent of a foreign power" and that the collection of foreign intelligence information is a "significant purpose" of the investigation. 50 U.S.C. § 1805(3)(A) (2006).

9. *See infra* Part I.C.2.

procedure—which requires probable cause to obtain a warrant—would be followed when ordinary law enforcement,[10] and not foreign intelligence, was the primary purpose of the electronic surveillance.[11]

The Patriot Act amended FISA[12] by eliminating the requirement that the government demonstrate that foreign intelligence surveillance is the "primary purpose" of the surveillance.[13] Under the amended FISA, the government may conduct electronic surveillance even when gathering foreign intelligence is merely a "significant purpose" of the surveillance.[14] The Patriot Act also expressly permits intelligence officers and law enforcement agencies to consult and coordinate information to investigate or protect against terrorist activity.[15] Whereas FISA originally restricted electronic surveillance to the investigation of foreign agents, these amendments allow the government to conduct FISA surveillance even when ordinary domestic criminal prosecution—and not foreign intelligence gathering—is its primary objective.[16] The information gathered through FISA surveillance could then be used against criminal defendants charged with a crime that is unrelated to foreign intelligence.[17]

In sum, the Patriot Act's amendments to FISA eradicated warrant and probable cause requirements for searches and seizures when the primary purpose of surveillance is ordinary law enforcement. FISA, as amended by the Patriot Act, became exactly what the original legislation was intended *not* to be: an alternative to

10. For the purposes of this Note, the terms "ordinary crimes" or "ordinary criminal prosecutions" will refer to those crimes or prosecutions that are unrelated to foreign intelligence, national security, or terrorism.

11. Banks, *supra* note 7, at 1241.

12. Although Congress amended FISA several times, first in 2001 and again in 2004, 2007 and 2008, the later amendments do not affect the problem addressed by this Note. Accordingly, the amendments to FISA discussed here were enacted in 2001.

13. Although Congress amended FISA several times, first in 2001 and again in 2004, 2007 and 2008, the later amendments do not affect the problem addressed by this Note. Accordingly, the amendments to FISA discussed here were enacted in 2001.

14. 50 U.S.C. §§ 1804(a)(7)(B),1805(a)(3)(A) (2006).

15. 50 U.S.C. § 1806(k)(1)(A)–(C) (2006) (expressly permitting federal officers gathering intelligence under FISA to "consult with Federal law enforcement officers . . . to coordinate efforts to investigate or protect against" sabotage, international terrorism, espionage or other grave hostile acts by foreign powers or their agents).

16. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 613 (Foreign Intel.Surv.Ct. 2002) [hereinafter *In re* All Matters].

17. William Pollak, *Shu'ubiyya or Security? Preserving Civil Liberties by Limiting FISA Evidence to National Security Prosecutions*, 42 U. MICH. J.L. REFORM 221, 222–23 (2008).

traditional criminal procedure, circumventing constitutional requirements in order to build a criminal case against a domestic defendant with slight or non-existent ties to a foreign power.[18] Through the amended FISA's new grant of authority to the Executive to conduct such sweeping surveillance, Congress has reincarnated the reviled general warrants of the eighteenth century.

This Note argues that the use of evidence procured through FISA surveillance against defendants charged with crimes unrelated to the purpose of the FISA authorization—that is, foreign intelligence gathering—violates the Fourth Amendment because the seizure and subsequent use of the evidence goes beyond the scope of a constitutionally permitted search. Under the amended FISA, the executive is required to certify that foreign intelligence is a "significant purpose" of the surveillance.[19] Thus, the use of evidence gathered during the FISA surveillance in ordinary criminal prosecutions—which are, by definition, unrelated to this "significant purpose"—demonstrates that the scope of such a warrant is unreasonably broad.

This Note then proposes a solution: the return of the mere evidence rule as a limit on the use of FISA evidence in ordinary criminal prosecutions. The mere evidence rule, articulated by the Supreme Court in *Gouled v. United States* in 1921, once defined the constitutional scope of a search and seizure.[20] Under this rule, law enforcement officials were not permitted to search and seize items solely for the purpose of acquiring evidence—"mere evidence"—to be used against a defendant in a criminal proceeding.[21] Rather, law enforcement officials could only legally search and seize contraband or instrumentalities or fruits of a crime.[22]

When applied to FISA cases, this rule would serve as a judicial tool to strike the balance between the government's interest in law enforcement and the individual's right to privacy. Under this rule, any evidence unrelated to foreign intelligence purpose of the FISA warrant would constitute "mere evidence" and would be suppressed. By suppressing such evidence, the rule would deter government

18. Banks, *supra* note 7, at 1215.

19. *See supra* note 8.

20. Gouled v. United States, 255 U.S. 298, 309 (1921).

21. *Id.* at 299.

22. *Id.* at 309.

overreaching and compensate the individual for the violation of his or her constitutional rights.

Part I of this Note examines the history of electronic surveillance jurisprudence, analyzes the Supreme Court decisions that led to the enactment of FISA, and discusses the Patriot Act's amendments to FISA. Part II frames the constitutional problem posed by the amendments. Part III analyzes the constitutional argument against using the fruits of FISA surveillance against defendants charged with ordinary crimes. Part IV proposes that a limit on the use of FISA evidence be imposed in the form of the mere evidence rule, and discusses the recent en banc Ninth Circuit opinion that applies a similar rule, albeit in a different context, to address a problem similar to the one discussed in this Note.

I. The History of National Security Surveillance

A. The Origins of the Fourth Amendment and Its Application to National Security Surveillance

1. The Birth of the Fourth Amendment

The Fourth Amendment to the United States Constitution clearly expresses the Framers' wish to keep private homes free from government invasion.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons and things to be seized.[23]

The Fourth Amendment was the constitutional protection against the evils of the general warrant—a British procedure, sanctioned by law, whereby writ-bearing agents of the Crown broke down the doors of suspected dissidents in order to perform searches.[24] These searches were not constrained, as authorities were generally free to "break into any shop or place suspected" and seize anything.[25]

23. U.S. CONST. amend. IV.

24. William Cuddihy & B. Carmon Hardy, *A Man's House Was Not His Castle: Origins of the Fourth Amendment to the United States Constitution*, 37 WM. & MARY Q. 371, 372 (1980).

25. *Id.* at 381 (quoting a 1621 Privy Council general warrant).

The general warrants were used to intimidate dissidents, authors, and printers of seditious materials.[26] They were used to enforce excise laws and seize excised goods,[27] enforce customs laws,[28] and impose taxes.[29]

The English methods of search and seizure were used just as frequently in the American colonies as they were in Britain.[30] Through writs of assistance—the colonial equivalent of the general warrant—authorities stormed through homes searching for taxable goods and contraband, and arresting escaped slaves and vagrants.[31] In many respects, the searches in America were more invasive than those in England because the British colonial government, which established the writs, generally discarded whatever few restraints there were on the general warrant.[32] As the searches grew more common and more invasive,[33] the colonists reacted violently, frequently responding to the searches by barring doors with axes and attacking the searchers with weapons.[34] Because colonial law failed to recognize a right of individual privacy, the colonists had no legal remedy for the invasion.[35]

Against this backdrop, the Founding Fathers crafted a constitution that would recognize the civil liberties largely ignored by the British crown. On June 8, 1789, James Madison proposed language to the Constitutional Convention that became the Fourth

---

26. Entick v. Carrington, 19 Howell's State Trials 1029, 1067 (1765), *available at* http://www.constitution.org/trials/entick/entick_v_carrington.htm.

27. Cuddihy & Hardy, *supra* note 24, at 383 (describing the usage of general warrants to impose taxes as "absolutely intolerable to private persons," and introducing dangerous precedent: "the practice of using general warrants would proliferate until the excise laws reached 'the domestic concerns of every private family, and . . . every species of produce in the land.'").

28. *Id.* at 384 (describing writs of assistance for customs authorities that "permitted bearers of such writs to 'enter and goe into any house, shop, celler, warehouse, or roome or other place, and in case of Resistance . . . to break open doores, chests, truncks, and other packages,' and to seize and impound illegal goods.").

29. *Id.* (A 1688 tax law authorized tax collectors "'to breake open in the day-time any House and upon Warrant . . . any chest, Trunck, or Box' containing tax-able articles. Similar powers were granted by statutes affecting military recruitment, naval impressment, and bankruptcy.").

30. *Id.* at 388.

31. *Id.* at 390.

32. *Id.*

33. *Id.* at 391–92.

34. *Id.*

35. William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 3 (2000).

Amendment.[36] The Convention, mindful of the evils of the writs of assistance, required specificity for warrants to search and seize. Over one hundred and seventy years later, the United States Supreme Court would require that same specificity in electronic invasions of privacy.[37]

2. The United States' Long History of Spying on Its Citizens

The history of government surveillance for the purpose of gathering intelligence stretches to the early days of the Revolutionary War, when the Continental Congress established the Committee for Secret Correspondence and enacted the first espionage legislation, which made it a capital crime for "all persons . . . [to be] found lurking as spies."[38] President George Washington, recalling his experience as an analyst and spymaster in the Revolutionary War, specifically requested funds for intelligence operations during his first State of the Union Address.[39] Congress complied.[40] Most of the presidents after Washington followed his model and assumed responsibility for covert foreign intelligence actions.[41] For the most part, Congress deferred to the President, believing that such power was vested in the Executive.[42]

In the 1930s, as the country prepared for war, the Federal Bureau of Investigation ("FBI"), under the direction of J. Edgar Hoover, started using electronic surveillance for national security purposes.[43] President Franklin Delano Roosevelt authorized J. Edgar Hoover to gather intelligence on persons "detrimental to the security of the United States," with a special emphasis on targeting individuals

36. *Id.*

37. *See* Katz v. United States, 389 U.S. 347, 357–59 (1967) (holding that a warrant, authorized by a neutral magistrate and possessing the required specificity and particularity, must be obtained before law enforcement officials can conduct electronic surveillance of a telephone conversation in a phone booth, even when officials have probable cause to believe that a crime is being or will be conducted); Osborn v. United States, 385 U.S. 323, 329–30 (1966) (holding that, under sufficiently "precise and discriminate circumstances," a federal court may authorize government officials to use a concealed electronic device "for the narrow and particularized purpose of ascertaining the truth of allegations" of a "detailed factual affidavit alleging the commission of a specific criminal offense").

38. Banks & Bowman, *supra* note 35, at 11–12.

39. *Id.* at 15.

40. *Id.* at 15.

41. *Id.* at 17.

42. *Id.* at 18.

43. *Id.* at 26.

suspected of espousing fascism or communism.[44] This unfettered executive power to gather intelligence in the name of national security expanded virtually unabated until the early 1970s.[45] By then, the FBI files were thick with personal information on private individuals, and the changing political climate brought public outcry at the activities of the intelligence community.[46]

In response to public pressure, Congress began to investigate intelligence activities in the United States. In 1975, the Senate commissioned the Select Committee to Study Governmental Operations with Respect to Intelligence Activities (known as the "Church Committee," after its Chair, Senator Frank Church).[47] The Church Committee found that every President since Roosevelt had violated individual privacy by conducting secret electronic surveillance without prior judicial approval.[48] Many targets of the surveillance were never suspected of criminal activity and were targeted solely for beliefs protected under the First Amendment.[49] For example, the Church Committee revealed that the government conducted warrantless surveillance of Martin Luther King and other civil rights leaders, as well as Vietnam War dissenters.[50] Following the Church Committee's report, Congress started regulating intelligence gathering.[51]

3. Applying the Fourth Amendment to Electronic Surveillance

Problems arise, however, when attempting to apply the Fourth Amendment—originally designed to combat overreaching searches in ordinary criminal law—to the area of national security surveillance, which seeks to address threats to our national security not contemplated at the time of its enactment. The Fourth Amendment is implicated by national security investigations because the methods used to investigate criminal enterprises are also used in gathering

44. *Id.*

45. *Id.* at 32–34.

46. *Id.*

47. *Id.* at 33; *see* Elizabeth Gillingham Daily, Comment, *Beyond 'Persons, Houses, Papers, and Effects': Rewriting the Fourth Amendment for National Security Surveillance*, 10 LEWIS & CLARK L. REV. 641, 645 (2006).

48. Daily, *supra* note 47, at 645.

49. *Id.* at 654.

50. *Id.*

51. *Id.*

intelligence.[52] Furthermore, the fact that information gathered during the course of a national security investigation may be turned over to officials for use in an ordinary criminal prosecution and introduced as evidence against a criminal defendant also implicates the Fourth Amendment.[53]

Despite the information overlap, national security investigations and ordinary law enforcement investigations are distinct creatures: each one serves a different purpose and protects different interests.[54] Ordinary law enforcement, through a criminal investigation, seeks to root out individual criminals and bring them to justice.[55] Furthermore, before electronic surveillance in the form of Fourth Amendment searches or seizures can take place, law enforcement officials must demonstrate to a neutral magistrate that they have probable cause to believe that their surveillance will expose evidence of a crime.[56]

On the other hand, national security investigations target general threats to national security and are based on standards much lower than the probable cause required in criminal investigations.[57] In order to stay one step ahead of an attack, national security investigations are undertaken before any criminal activity begins.[58] The purpose of such investigations is to prevent "unlawful activity or [enhance] the [g]overnment's preparedness for some possible future crisis or emergency," and not necessarily to secure a conviction for actual criminal activity.[59] Thus, the focus of intelligence gathering for national security purposes, "may be less precise"—and, as a result, more sweeping—"than that directed against more conventional types of crime."[60]

Because of these fundamental differences, courts have been more willing to bypass Fourth Amendment scrutiny in the area of national security than in the area of ordinary law enforcement.[61] Such

52. Banks & Bowman, *supra* note 35, at 4.

53. *Id.*

54. *Id.* at 7.

55. *Id.*

56. *Id.* at 8.

57. *Id.* at 9.

58. *Id.* at 8.

59. United States v. U.S. Dist. Ct., (Keith) 407 U.S. 297, 322 (1972).

60. *Keith*, 407 U.S. at 322.

61. *Id.* at 308, 321–22 (recognizing that there is no "question or doubt as to the necessity of obtaining a warrant in the surveillance of crimes unrelated to the national

leniency in the area of criminal procedure, especially when involving a foreign power or its agents, is grounded on the belief that a traditional warrant acquired from a neutral magistrate, as required by Rule 41 of the Federal Rules of Criminal Procedure,[62] might "unduly frustrate the efforts of government to protect itself from acts of subversion and overthrow directed at it."[63] In addition, as the Supreme Court recognized, the nature of intelligence gathering requires stealth and secrecy.[64] Consequently, traditional notice requirements of Rule 41 could undermine the purpose of the national security surveillance, as would the requirements of probable cause and particularity.[65] Thus, the Supreme Court has recognized that the traditional warrant required in ordinary law enforcement may not apply in national security surveillance.[66] Lower courts have also deferred to the President's designation as "the pre-eminent authority in [the area of] foreign affairs" and permitted warrantless searches in cases involving a foreign power or its agents. [67]

B. The Court's Role

The concept that the Fourth Amendment protects the right to privacy in addition to property first appeared at the end of the nineteenth century in *Boyd v. United States*.[68] *Boyd* involved the seizure of the defendant's papers—tangible, private property which the government sought to introduce as evidence against the defendant.[69] The Court held that the defendant's private papers were protected from search and seizure by the Fourth (and Fifth) Amendments because unless the government had a higher claim to the property in question—for example, if the government had probable cause to believe that the property was stolen or contraband—the government had no right to seize it.[70]

---

security interest," but that national security surveillance may involve "different policy and practical considerations from the surveillance of 'ordinary crime'").

62. *See* FED. R. CRIM. P. 41(b).

63. *Keith*, 407 U.S. at 315.

64. *Id.* at 319.

65. *Id.* at 322 (noting that the same types of standards and procedures prescribed by Title III need not necessarily be applicable in foreign intelligence gathering cases).

66. *Id.*

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

68. Boyd v. United States, 116 U.S. 616, 630 (1886).

69. *Id.*

70. *Id.*

Forty years later, in 1928, the Court denied an appeal to extend the Fourth Amendment's right to privacy to a case that did not involve physical property.[71] In *Olmstead v. United States*, the Court held that the government's electronic surveillance of the defendant was not a search or seizure under the Fourth Amendment because there was no actual physical invasion of the defendant's house.[72] The words of the Fourth Amendment itself, the Court reasoned, "show that the search is to be of material things—the person, his house, his papers, or his effects."[73] Because the government avoided any trespass on the defendant's property by wiretapping the phone lines using wires outside his house, the Fourth Amendment was not implicated.[74]

In his vigorous dissent, Justice Brandeis cautioned against adopting too literal an interpretation of the Fourth Amendment.[75] He argued that the protections guaranteed by the Fourth Amendment were "much broader in scope" than the majority had defined,[76] Rather than only protecting persons, papers, houses, and effects,

> [t]he makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the

71. Olmstead v. United States, 277 U.S. 438, 438 (1928).

72. *Id.* at 464.

73. *Id.* at 466 (noting that no federal court has held that the Fourth Amendment had been violated "unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure").

74. *Id.* at 466 ("The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment. Here those who intercepted the protected voices were not in the house of either party to the conversation.").

75. *Id.* at 472–79 (Brandeis, J., dissenting).

76. *Id.* at 478.

means employed, must be deemed a violation of the Fourth Amendment.[77]

Justice Brandeis further argued that the Fourth Amendment must also extend to the "subtler and more far-reaching means of invading privacy [that] have become available to the government."[78] The Constitution is "not [an] ephemeral enactment[], designed to meet passing occasions."[79] Rather, it is "designed to approach immortality as nearly as human institutions can approach it."[80] The Court, when interpreting the Constitution, must contemplate not "only . . . what has been but . . . what may be."[81] A flexible reading of the Constitution is vital to dealing with the invasions of "the sanctit[ies] of a man's home and the privacies of life" by methods yet unknown and unforeseen.[82]

Despite Justice Brandeis's powerful rhetoric, the *Olmstead* majority's narrow interpretation of the Fourth Amendment's reach remained the law when applied to the government's use of electronic surveillance until the Court reversed itself in *Katz v. United States*.[83] In *Katz*, the Court held that Fourth Amendment protections apply to electronic surveillance.[84] The Fourth Amendment "extends as well to the recording of oral statements overheard without any 'technical trespass . . . under local property law.'"[85] Overturning the holding in *Olmstead*, the Court rejected the idea that the Fourth Amendment applied only to unreasonable search and seizure of tangible items: "the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given

77. *Id.*

78. *Id.* at 473.

79. *Id.* (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

80. *Id.* (internal quotation marks omitted).

81. *Id.*

82. *Id.* (alteration in original) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)). In espousing a flexible reading of the Constitution, Brandeis cautioned that "'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." *Id.*

83. Katz, 389 U.S. at 351–53.

84. *Id.* at 353.

85. *Id.* (citation omitted).

enclosure."[86] Instead, the principal factor in whether an act of the government constituted a search or seizure under the Fourth Amendment lay not in the physical location of the action, but in whether the individual had a "reasonable expectation of privacy" in the circumstances.[87]

Although the Court's decision limited the government's ability to conduct electronic surveillance, the Court refused to address the power of the executive to conduct electronic surveillance for national security purposes.[88] In his concurrence, Justice White argued that there should be an exception to the warrant requirement for national security surveillance.[89] On the other hand, Justice Douglas, who concurred in the judgment, wrote a separate concurrence to address the words of Justice White.[90] According to Justice Douglas, Justice White's espousal of an exception to the warrant requirement for national security was a "wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping in cases which the Executive Branch itself labels 'national security' matters."[91] The warrant requirement should most certainly apply in those situations because neither the President nor the Attorney General is "detached, disinterested, and neutral as a court or magistrate must be."[92] Rather, they are "properly interested parties, cast in the role of adversary, in national security cases."[93] Justice Douglas' rejection of an exception to the warrant requirement for national security matters arguably supports the view that the courts play a vital role in mediating between the competing interests of law enforcement and the privacy of the individuals targeted by national security wiretaps.[94] These two competing views persist to this day in the debate over national security surveillance.

86. *Id.*

87. *Id.* at 360–61 (Harlan, J., concurring).

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

89. *Id.* at 363–64 (White, J., concurring) ("We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirement of national security and authorized electronic surveillance as reasonable.").

90. *Id.* at 359 (Douglas, J., concurring).

91. *Id.*

92. *Id.*

93. *Id.* at 360.

94. *Id.*

C. Congressional Regulation of Electronic Surveillance and the Diminishing Role of the Courts

1. Title III and the Keith *Case*

After *Katz*, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III") to regulate the use of electronic surveillance in law enforcement investigations.[95] Title III established a warrant procedure that closely tracked the Court's ruling in *Katz*. For example, Title III requires a law enforcement officer to submit an oath or affirmation to a judge[96] describing the facts giving rise to "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense."[97] The judge must also find probable cause to believe that surveillance is *necessary* to obtain evidence of a crime, and that the facility being targeted by surveillance is being used in connection with the crime or by the person suspected of the crime.[98] Finally, the judge must determine that "normal investigative procedures" other than electronic surveillance were unsuccessful or unreasonable.[99] Only then will the judge grant a surveillance warrant.[100]

The statute also contains several provisions that minimize the invasion of privacy even after the warrant is issued. For example, surveillance orders are limited to thirty days, although an extension may be granted upon re-application.[101] Furthermore, the target of the surveillance must be notified of the surveillance within ninety days of its termination.[102] This notice requirement is significant because, as discussed below, the notice requirements for FISA differ significantly.[103]

However, Congress explicitly exempted foreign surveillance from the limits imposed on ordinary law enforcement investigations by Title III. The statute specifically states that:

---

95. 18 U.S.C. §§ 2516–2518 (2006).

96. § 2518(1).

97. § 2518(3)(a). The statute further requires that the suspected crime be one of those enumerated under section 2516(1). *Id.*

98. § 2518(3)(b)–(d).

99. § 2518(3)(c).

100. § 2518(3). The statute further requires that the suspected crime be one of those enumerated under section 2516(1). *Id.*

101. § 2518(5).

102. § 2518(8)(d).

103. *See infra* Part I.C.3.

> 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 Unites 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.[104]

In *United States v. United States District Court*—commonly known as the *Keith* case[105]—the Supreme Court applied the Fourth Amendment to domestic surveillance.[106] The Court held that the government may not conduct domestic surveillance, electronic or otherwise, without a warrant.[107]

In *Keith*, the government charged one of the defendants with the bombing of a CIA office in Ann Arbor, Michigan.[108] During the trial, the government admitted that it had conducted warrantless electronic surveillance of the defendant, but argued that it was nonetheless legal because the purpose of the surveillance—"to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of Government"—justified an exception to the warrant requirement.[109] The Court rejected the government's argument and held that the facts of *Keith* did "not justify complete exemption of domestic security

104. United States v. U.S. Dist. Ct., (Keith) 407 U.S. 297, 302–03 (1972) (quoting 18 U.S.C. § 2511(3) (1976), *repealed by* Foreign Intelligence Surveillance Act of 1978).

105. The title of this case, *Keith*, "is taken from the name of then-United States District Court Judge Damon Keith. Interestingly, Judge Keith was not the original judge in the case. 'The case was originally assigned to United [States] District Court Judge Talbot Smith, but was randomly reassigned to Judge Keith when Smith recused himself for personal reasons.'" Tracey Maclin, *The Bush Administration's Terrorist Surveillance Program and the Fourth Amendment's Warrant Requirement: Lessons From Justice Powell and the Keith Case*, 41 U.C. DAVIS L. REV. 1259, 1263 (2008) (citation omitted).

106. *Keith*, 407 U.S. at 297.

107. *Id.*

108. *Id.* at 299.

109. *Id.* at 300.

surveillance from prior judicial scrutiny."[110] When conducting electronic surveillance for domestic security purposes, the Court held, the Fourth Amendment requires that the government first seek judicial approval from a neutral magistrate.[111]

The Court reached this conclusion by balancing the government's duty "to protect the domestic security [against] the potential danger posed by unreasonable surveillance to individual privacy and free expression."[112] The Court established a framework to guide lower courts' determination of the issue:

> If the legitimate need of Government to safeguard domestic security requires the use of electronic surveillance, the question is whether the needs of citizens for privacy and [the] free expression may not be better protected by requiring a warrant before such surveillance is undertaken. We must also ask whether a warrant requirement would unduly frustrate the efforts of [the] Government to protect itself from acts of subversion and overthrow directed against it.[113]

While recognizing the "constitutional basis of the President's domestic security role," the Court held that it "must [nonetheless] be exercised in a manner compatible with the Fourth Amendment."[114] By requiring a warrant prior to initiating surveillance, the risk of violating individual privacy and freedom of expression would be avoided.[115]

The Court, however, limited its holding in two ways. First, it noted that its decision in *Keith* involved only "the domestic aspects of national security," and refused to address "the issues which may be involved with respect to activities of foreign powers or their agents."[116] Second, the Court stated that although the Fourth Amendment requires the government to obtain a warrant prior to initiating surveillance for national security purposes, "domestic security

110. *Id.* at 320.

111. *Id.*

112. *Id.* at 315.

113. *Id.*

114. *Id.* at 320.

115. *Id.* at 318 ("Prior review by a neutral and detached magistrate is the time-tested means of effectuating Fourth Amendment rights.").

116. *Id.* at 321–22.

surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.'"[117]

The Court's limiting words are important because they created a distinction between surveillance for the purpose of gathering information on domestic threats to national security and surveillance for information on ordinary crime which previously did not exist.[118] The Court stopped short of offering real guidance, however, in failing to define the distinction in terms of the type of threat required or the government interest involved. Furthermore, although the Court permitted a warrant requirement for domestic security surveillance, which was different from those required by Title III,[119] the Court did not specify what type of differences would be constitutionally permissible.[120]

2. *Applying* Keith *to Foreign Intelligence Surveillance and the Birth of the Primary Purpose Test*

Most federal circuit courts of appeal interpreted the hole left by the Supreme Court in *Keith* to mean that foreign intelligence surveillance, unlike domestic security surveillance, justified an exception to the warrant requirement.[121] The most prominent case

117. *Id.* at 322.

118. *See* Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and The Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319, 331 (2005).

119. *Keith*, 407 U.S. at 322 ("[W]e do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case.").

120. *See* Seamon & Gardner, *supra* note 118, at 332 ("[T]he *Keith* opinion suggests that the Fourth Amendment varies in stringency, requiring the most strict procedures and standards for electronic surveillance of 'ordinary crime' (the subject of Title III); less strict procedures and standards—which nonetheless generally include prior judicial approval—for electronic surveillance for information related to domestic threats to national security (the subject of *Keith* itself); and the least strict procedures and standards for electronic surveillance for foreign threats to national security (the context as to which the *Keith* Court expressly reserved decision).").

121. *See, e.g.*, United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977) (holding that the Fourth Amendment permits warrantless surveillance as long as in camera review reveals that the purpose of the surveillance is to gather foreign intelligence information); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (holding that the Fourth Amendment permits warrantless surveillance as long as its sole purpose is to gather foreign intelligence information and any retention of evidence of criminal activity is incidental); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) (holding that the Fourth Amendment permits warrantless surveillance so long as the purpose of the surveillance is to gather intelligence information).

addressing this issue is *United States v. Truong Dinh Hung*.[122] In *Truong*, the defendant, an American citizen, was convicted of transmitting classified information to representatives of the Socialist Republic of Vietnam during the 1977 Paris negotiations between that country and the United States.[123] The defendant moved to suppress the prosecution's use of evidence gained through warrantless electronic surveillance on the ground that it constituted an unreasonable search under the Fourth Amendment.[124] The government argued that the special circumstances of foreign intelligence justified a warrant exception to the Fourth Amendment.[125]

The district court accepted the government's argument that the Fourth Amendment's warrant requirement contained an exception for the collection of foreign intelligence.[126] However, the court held that the exception should be limited to those cases where the Executive was conducting "primarily" a foreign intelligence investigation.[127] Accordingly, the district court admitted evidence against the defendant that was gathered "during the period the investigation primarily concerned foreign intelligence," but excluded evidence when it determined that the investigation became "primarily a criminal investigation."[128]

The Fourth Circuit affirmed.[129] Using the *Keith* balancing framework, the *Truong* court found that the needs of the Executive "are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . 'unduly frustrate' the President in carrying out his foreign affairs responsibilities."[130] But recognizing that individual privacy rights are severely compromised when the government conducts surveillance without judicial authorization, the court stressed that the foreign

122. United States v. Truong Dinh Hung, 629 F.2d 908, 915 n.4 (4th Cir. 1980). Although *Truong* was decided after the enactment of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), the government surveillance took place in 1977, so the court did not apply FISA.

123. *Id.* at 911–12.

124. *Id.* at 912.

125. *Id.*

126. *Id.*

127. *Id.* at 912–13.

128. *Id.* at 913.

129. *Id.*

130. *Id.*

intelligence exception to the warrant requirement was limited to those cases where the government's interests "are paramount."[131] The government's interests are "paramount"—that is, they are so compelling that it should be relieved of seeking a warrant—only when two conditions are met: First, when "the object of the search or the surveillance is a foreign power, its agents or collaborators"; and second, when the surveillance is conducted "primarily for foreign intelligence reasons."[132] These conditions ensured that even foreign actors and their agents would "receive the protection of the warrant requirement if the government is primarily attempting to put together a[n] [ordinary] criminal prosecution."[133]

In reaching this conclusion, the court distinguished between warrantless surveillance for the purpose of gathering foreign intelligence and surveillance for the purpose of ordinary criminal prosecution.[134] First, unlike an ordinary criminal investigation, foreign intelligence surveillance entails "the utmost stealth, speed, and secrecy."[135] Requiring the President to obtain a warrant before conducting surveillance would risk delaying the response to terrorist threats and leaking of sensitive information.[136] Second, the judiciary is not competent in the field of intelligence and should defer to the Executive's expertise.[137] Finally, the Executive not only has the expertise, but has been "constitutionally designated as the pre-eminent authority in foreign affairs."[138] Thus, the special circumstances surrounding foreign intelligence justified a departure from traditional Fourth Amendment principles.

The *Truong* court's decision came to be known as the "primary purpose test,"[139] which played an important role in national security jurisprudence, even after the enactment of FISA.

131. *Id.* at 915.

132. *Id.*

133. *Id.* at 916.

134. *Id.*

135. *Id.* at 913.

136. *Id.*

137. *Id.*

138. *Id.* at 914.

139. Seamon & Gardner, *supra* note 118, at 364-64 (noting that *Truong* "deserves credit as the progenitor of the 'primary purpose' test that became associated with the FISA").

3. The Foreign Intelligence Surveillance Act of 1978

In 1978, in the wake of the Watergate scandal and the Church Committee reports, the Ninety-Fifth Congress enacted the Foreign Intelligence Surveillance Act to regulate the Executive Branch's use of electronic surveillance.[140] Using the Supreme Court's very words from *Keith*, FISA authorized the government to conduct electronic surveillance of "foreign powers" and "agents of foreign powers" for "the purpose" of gathering "foreign intelligence information" so long as the government received prior judicial approval.[141] FISA thus established a new court, called the Foreign Intelligence Surveillance Court ("FISC"), whose sole jurisdiction is limited to hearing applications and granting orders for electronic surveillance of such foreign powers.[142] FISA also established an appellate court, the Foreign Intelligence Surveillance Court of Review ("FISCR"), whose sole jurisdiction is limited to reviewing the denial of any FISA application.[143] The FISCR has heard only one case in the history of its existence.[144]

Although FISA established some limitations on the government's ability to conduct electronic surveillance, it differed markedly from Title III procedures. The most glaring difference was

---

140. *Id.* at 337.

141. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801-11 (2000), 18 U.S.C. §§ 2511, 2518-19 (2000)), amended by USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended at 50 U.S.C.A. §§ 1801-11, 18 U.S.C.A. §§ 2511, 2518-19). In 2001, the Patriot Act amended FISA to require that applicants certify that "a significant purpose"—instead of "the purpose"—of the surveillance is gathering foreign intelligence information. Foreign intelligence information is:

> (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.

50 U.S.C. § 1801(e) (2006).

142. 50 U.S.C. § 1803(a) (2006).

143. 50 U.S.C. § 1803(b).

144. *In re* Sealed Case, 310 F.3d 717, 717 (Foreign Int. Surv. Ct. Rev. 2002).

FISA's departure from the traditional warrant requirements implemented by Congress in Title III to comply with the Fourth Amendment. Under Title III, a court will issue a warrant for electronic surveillance only when the government demonstrates that there is probable cause that a crime has occurred, and that a particular individual was involved.[145] Title III's probable cause requirement discouraged the government from using electronic surveillance to investigate persons for whom the government lacked probable cause—or even reasonable suspicion—of criminal activity. FISA, however, requires only that a federal officer certify that the target is a foreign power or its agent, and that "a significant purpose of the surveillance is to obtain foreign intelligence information" that cannot be obtained through normal investigative techniques.[146]

Another difference between FISA and traditional Title III procedures is the extent to which the reviewing judge may challenge and evaluate the substance of the federal officer's certification, probing for illegalities or insufficiencies. FISA requires the FISC to approve an order for surveillance "as requested or as modified" if the court determines that the target of the surveillance is a foreign power or agent of a foreign power.[147] The FISC judge may not review the agent's certification that the purpose of the surveillance is to obtain foreign intelligence information.[148] It does so only if the target of the surveillance is a U.S. citizen, and, even then, the court will review the government's certification of a foreign intelligence purpose for clear error only.[149] The clear error standard is so deferential to the government that judges have interpreted it to discourage them from second guessing the government's claims of a foreign intelligence purpose.[150] This deference has also led courts to largely ignore the

145. 18 U.S.C. § 2518(3)(a) (2006). Title III also requires that the applicant was unsuccessful at all other investigative techniques before seeking a surveillance warrant, § 2518(3)(c), which is absent in FISA. Title III thus requires the government to use electronic surveillance only as a last resort when all other investigatory techniques have failed. *See* § 2518(1)(c) (requiring the Title III warrant application to state "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous").

146. 50 U.S.C. § 1804(a) (2006).

147. 50 U.S.C. § 1805 (a)(3)(A)–(B) (2006).

148. 50 U.S.C. § 1805(a)(5).

149. *Id.*

150. United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984).

exclusionary rule in FISA cases,[151] and to refuse to suppress FISA evidence even when falsehoods in the FISA application were exposed.[152] The judiciary was thus relegated to the task of merely evaluating whether the FISA application complied with the statutory requirements.

Finally, FISA differed from Title III in terms of the length of the surveillance and of the notice requirements. Under Title III, surveillance was limited to thirty days,[153] while FISA surveillance may be authorized for up to one hundred twenty days.[154] Furthermore, Title III requires that targets be notified of the surveillance ninety days after termination of the surveillance,[155] while FISA targets are provided notice after-the-fact only if the intercepted communications are sought to be admitted in a criminal proceeding.[156] Despite this right to limited after-the-fact disclosure, defendants have been unable to mount an adequate motion to exclude because they do not have access to the government's information that led to its application for surveillance, contained in materials such as the application itself, the

151. 50 U.S.C. § 1806(g) (2006) ("If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure."). *But see* United States v. Mazook, 435 F. Supp. 2d 778, 788–91 (N.D. Ill. 2006) (refusing to suppress evidence obtained during physical search of defendant's home which was unauthorized by the version of FISA in force at the time); United States v. Bin Laden, 126 F. Supp. 2d 264, 282–84 (S.D.N.Y. 2000), *aff'd*, United States v. Bin Laden, No. S7R 98CR1023KTD, 2005 WL 287404, at *9–11 (S.D.N.Y. Feb. 7, 2005) (FISA evidence admissible despite government's failure to obtain proper authorization from Attorney General until eight months into surveillance); United States v. Ajlouny, 629 F.2d 830, 839–40 (2d Cir. 1980) (refusing to suppress evidence from unlawful surveillance on ground that exclusionary rule did not apply).

152. *See, e.g.*, United States v. Daly, Nos. 05-10718, 05-10719, 05-10728, 05-10729, 2007 WL 2212362, at *1 (9th Cir. Aug. 2, 2007) ("Even if the statements that [defendant] points to in the affidavit supporting the search warrant for his home and office were false, he failed to make a substantial preliminary showing that the affidavit's remaining content is insufficient to establish probable cause.").

153. 18 U.S.C. § 2518(5) (2006).

154. 50 U.S.C. § 1805(e)(1) (2006).

155. 18 U.S.C. § 2518(8)(d).

156. 50 U.S.C. §§ 1802(a)(3), 1806(c)–(d). *Compare* 18 U.S.C. § 2518(9) *and* §2516(1) *with* § 1806(f)–(g) (2006). Also, the FISC meets in secret, at an undisclosed location, and does not publish its decisions and its orders are sealed. § 1806(f).

certification, and affidavits.[157] Indeed, not a single defendant has been able to successfully challenge a FISA application because courts have refused to order the disclosure of a FISA application to a criminal defendant.[158]

The lower courts are split on whether FISA procedures comply with the Fourth Amendment. Some courts have held that the FISA procedures meet the Fourth Amendment's requirements of judicial authorization and particularity. For example, in *United States v. Sarkissian*, the Ninth Circuit held that compliance with FISA procedures satisfied the Fourth Amendment and cautioned against drawing too fine a distinction between investigations for criminal purposes as opposed to investigations for foreign intelligence purposes, because one inherently involved the other.[159] On the other hand, in *United States v. Duggan*, the Second Circuit adhered to the primary purpose test of *Truong*, holding that electronic surveillance complied with the Fourth Amendment only when the primary purpose of the investigation was foreign intelligence.[160]

4. The Primary Purpose Test Evolves into 'The Wall'

The Department of Justice ("DOJ") adhered to the primary purpose test, which it interpreted as prohibiting criminal prosecutors from directing or controlling FISA investigations.[161] Thus, the DOJ adopted procedures that limited contact between federal foreign intelligence agents and federal prosecutors, fearing that communications between the intelligence officers and federal prosecutors would lead courts to exclude evidence on the ground that

157. *See* John D. McKinnon, *Volatile Formula: How Patriot Act Helped Convict Man in Baby-Food Ring—Mr. Jammal Faces 10 Years After Terror-Probe Tapes Are Used in Criminal Trial—A 14-Minute Rant Against U.S.*, WALL ST. J., April 4, 2006, at A1 ("Armed with a [FISA] warrant, authorities can eavesdrop on any conversation, regardless of whether it involves a crime. They can withhold from defendants the basis for issuing the warrant, hindering legal challenges to the FISA evidence. And they can restrict defendants' access to the classified transcripts and tapes, which makes it harder for the defense to parry the government's charges or mount its own case.").

158. *See* United States v. Sattar, No. 02 Cr. 395, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003) (listing cases where the courts have not ordered disclosure of the FISA application materials).

159. United States v. Sarkissian, 841 F.2d 959, 964–65 (9th Cir. 1988).

160. United States v. Duggan, 743 F.2d 59, 77–78 (2d Cir. 1984).

161. Seamon & Gardner, *supra* note 118, at 383–84.

the purpose of the investigation was primarily criminal prosecution.[162] These restrictions eventually became known as "the wall."[163]

The wall attracted public and Congressional attention after the terrorist attacks of September 11.[164] The media reported that intelligence and law enforcement agencies had information that they had failed to share among themselves in a way that might have prevented the attacks.[165] Congress hastily passed The Patriot Act in part to tear down the wall once and for all, by amending FISA to require only that the gathering of foreign intelligence information must be "a significant purpose"—as opposed to "*the* purpose"—of the surveillance.[166] FISA also authorized foreign intelligence officers to consult and coordinate with federal law enforcement officers.[167] The DOJ interpreted the Patriot Act amendments to mean that it was now permitted to conduct FISA surveillance even when the investigation was primarily concerned with ordinary criminal prosecution, so long as foreign intelligence gathering remained "a significant purpose."[168] Based on this interpretation, the DOJ established new "Intelligence Sharing Procedures," which permitted extensive information-sharing between "the FBI and the Criminal Division regarding, among other things, "the initiation, operation, continuation, or expansion of FISA searches or surveillance."[169] The FISC rejected the new procedures offered by the DOJ, holding—in a rare public opinion that was issued pursuant to an appeal—that the Patriot Act's amendments to FISA did not intend to destroy the wall.[170]

5. *FISCR Finally Tears Down 'The Wall'*

The DOJ's appeal of the FISC's ruling was the FISCR's first and, to this day, only case.[171] The issue before the FISCR was whether the

162. *Id.* at 323.

163. *Id.*

164. *Id.* at 323-24.

165. *See* Rogers & Cloud, *supra* note 3.

166. Seamon & Gardner, *supra* note 118, at 324. *See also* 50 U.S.C. § 1804(a)(7)(b) (2006).

167. 50 U.S.C. § 1806(k) (2006).

168. Seamon & Gardner, *supra* note 118, at 382.

169. Memorandum from John Ashcroft, U.S. Att'y Gen., to Director, FBI (Mar. 6, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/ag03/06/02.html. *See also* Seamon & Gardner, *supra* note 118, at 382–83.

170. *In re* All Matters, 218 F. Supp. 2d 611, 623–25 (Foreign Intel. Surv. Ct. 2002).

171. *In re Sealed Case*, 310 F.3d at 719.

primary purpose test applied to FISA surveillance in light of the Patriot Act's amendments to FISA.[172] The court found that the Patriot Act's "significant purpose" amendment to FISA allowed federal prosecutors to use FISA evidence for the purpose of prosecuting ordinary criminal activity so long as foreign intelligence was involved.[173] Neither the Constitution nor the amended FISA required the primary purpose test because it was based on a "false dichotomy" between foreign intelligence information and ordinary law enforcement evidence.[174] Thus, if the government's purpose "articulates a broader objective than criminal prosecution—such as the stopping an ongoing conspiracy—and includes other potential non-prosecutorial responses, the government meets the statutory test."[175]

II. Framing the Problem

The consequences of the FISCR's decision are clear: There is now virtually no difference between ordinary criminal law enforcement and intelligence gathering. So long as the Executive can articulate a significant foreign intelligence purpose for the investigation, it may also use the investigation to collect evidence for an ordinary criminal prosecution. The Executive's certification that the surveillance is for a significant foreign intelligence purpose is not reviewable by the FISC under any other standard than clear error. Consequently, this lower standard creates a way around the Fourth Amendment, allowing prosecutors to replace the higher Title III standards with FISA, thereby avoiding Title III's constitutionally mandated protections.

In response to this fortuitous switch, prosecutors got busy: from 2003 to 2004, "for the first time, the number of secret surveillance warrants issued in federal terrorism and espionage cases . . . exceeded the total number of wiretaps approved in criminal cases nationwide."[176] Even the FISC has noted that the increased information sharing between intelligence officials and criminal

172. *Id.* at 720.

173. *Id.* at 734–35 (finding that the Patriot Act's amendments to FISA permitted surveillance "even if 'foreign intelligence' is only a significant—not a primary—purpose").

174. *Id.* at 735.

175. *Id.*

176. Dan Eggen & Susan Schmidt, *Data Show Different Spy Game Since 9/11*, WASH. POST, May 1, 2004, at A1, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A57859-2004Apr30?language=printer.

prosecutors "appear[s] to be designed to amend the law and substitute FISA for Title III electronic surveillances and [Federal] Rule [of Criminal Procedure] 41 searches . . . because the government is unable to meet the substantive requirements of these law enforcement tools."[177] Thus, the amended FISA permits law enforcement officials to conduct more sweeping surveillance than under criminal law (i.e., Title III), on a lower showing of cause, and then use the fruits of the surveillance to prosecute a defendant for crimes unrelated to foreign intelligence.

The new FISA opens the door to potential abuse of the Fourth Amendment by the Executive. For example, because the requirement that the FISC find probable cause that the target is a "foreign power" or its agent is easily satisfied,[178] the new FISA makes it easier for law enforcement officials to use national foreign intelligence gathering pretextually, when the real goal of the surveillance is ordinary law enforcement. Under FISA, the definition of a "foreign power" is so broad that large swaths of the population would fit this description—including any component of a foreign government, a foreign political organization, or any entity that is directed or controlled by a foreign government.[179] The "incredible breadth" of the definitions in FISA also "include[s] definitions of criminal behavior so broad, as to encompass any violation of the criminal statutes of the United States . . . or any State."[180] These new provisions make it easier for the government to prosecute minority groups, immigrants, or political opponents merely on the basis of a tenuous connection to a foreign power.[181] Furthermore, the courts

177. *In re* All Matters, 218 F. Supp. 2d 611, 623 (Foreign Intel. Surv. Ct. 2002).

178. United States v. Truong Dinh Hung, 629 F.2d 908, 915–16 (4th Cir. 1980).

179. 50 U.S.C. § 1801(a) (2006).

180. Michael P. O'Connor & Celia Rumann, *Going, Going, Gone: Sealing the Fate of the Fourth Amendment*, 26 FORDHAM INT'L L.J. 1234, 1258 (2003).

181. For example, the Patriot Act's "lone wolf" provision makes any non-citizen who is acting alone a potential "agent of a foreign power." Before Congress amended FISA to include this provision, FISA previously required the government to show that the activities of a target of a FISA investigation were performed "for or on behalf of" a foreign power. 50 U.S.C. § 1801(b)(2)(C). The "lone wolf" provision essentially eliminated the required link between the target's activities and a foreign power or agent of a foreign power by broadening the definition of "agent of a foreign power" to include any non-U.S. person who "engages in international terrorism or activities in preparation therefor." 50 U.S.C § 1801(b)(1)(C). *See also* Statement of US Senator Russ Feingold on the Intelligence Reform Conference Report for the Congressional Record, (Dec. 8, 2004), *available at* http://feingold.senate.gov/statements/04/12/2004C09828.html. In his Statement on the Intelligence Reform Conference Report for the Congressional Record, United

have been deprived of their check on the Executive's certification that foreign intelligence is a significant purpose of the surveillance and that the target is a foreign power or its agent.[182]

The solution proposed by this Note is a limit on the use of evidence that is unrelated to a significant foreign intelligence purpose. This "use limit" would function as a rebirth of the mere evidence rule: Unrelated "mere evidence" must be suppressed in a criminal proceeding because the use of FISA fruits against a defendant

---

States Senator Russ Feingold stated that the "lone wolf" provision "eliminates the requirement in [FISA] that surveillance or searches be carried out only against persons suspected of being agents of foreign powers or terrorist organizations." Senator Feingold went on to say:

> Mr. President, I am troubled by some provisions that were added in conference that have nothing to do with reforming our intelligence network. The bill includes in section 6001 what has come to be known as the "lone wolf" provision. The lone wolf provision eliminates the requirement in the Foreign Intelligence Surveillance Act ("FISA") that surveillance or searches be carried out only against persons suspected of being agents of foreign powers or terrorist organizations. I am very concerned about the implications of this provision for civil liberties in this country.
>
> It is important to remember that FISA itself is an exception to traditional constitutional restraints on criminal investigations, allowing the government to gather foreign intelligence information through wiretaps and searches without having probable cause that a crime has been or is going to be committed. The courts have permitted the government to proceed with surveillance in this country under FISA's lesser standard of suspicion because the power is limited to investigations of foreign powers and their agents. This bill therefore writes out of the statute a key requirement necessary to the lawfulness of intrusive surveillance powers that may very well otherwise be unconstitutional.
>
> By allowing searches or wiretaps under FISA of persons merely suspected of engaging in or preparing to engage in terrorism, the bill essentially eliminates the protections of the Fourth Amendment. I voted against the lone wolf bill when it passed the Senate early in this Congress. I believe there are better and more constitutional ways to deal with a situation where evidence of a connection to a foreign government or terrorist organization is not easily obtained.
>
> Even if section 6001 survives constitutional challenge, it would mean that non-U.S. persons could have electronic surveillance and searches authorized against them using the lesser standards of FISA even though there is no conceivable foreign intelligence aspect to their case. This provision may very well result in a dramatic increase in the use of FISA warrants in situations that do not justify such extraordinary government power.
>
> If the government comes to the conclusion that an individual is truly acting on his or her own, then our criminal laws concerning when electronic surveillance and searches can be used are more than sufficient. True lone wolf terrorists can and should be investigated and prosecuted in our criminal justice system. Section 6001 allows the government to use FISA to obtain a warrant for surveillance even if it knows that the subject has no connection whatsoever with a foreign power or a terrorist organization. That is not right.). *See also* H.R. Rep. No. 108-796, (2004) (Conf. Rep.).

182. United States v. Rahman, 861 F. Supp. 247, 250 (S.D.N.Y. 1994) (holding that it is "not the function of the FISA court judge nor is it the function of this judge to 'second-guess' these certifications" (citing United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984))).

charged with ordinary crimes exceeds the scope of a legitimate FISA search. A FISA search for unrelated evidence is analogous to the general warrant or writs of assistance that the Fourth Amendment was meant to stem. In making this argument, this Note advocates that the use of evidence from a FISA search be limited to the purpose set forth in the statute: that foreign intelligence be a "significant purpose" of the surveillance.

III. Constitutional Arguments for a Use Limit on Evidence Acquired Under FISA

The Supreme Court has consistently held that the scope of a search, whether or not it is conducted with a warrant, must strictly comport with and be justified by the circumstances permitting its initiation.[183] Under FISA, as amended by the Patriot Act, the Executive must certify that "a significant purpose of the surveillance" is foreign intelligence.[184] When the government uses evidence that is unrelated to gathering foreign intelligence in order to convict a defendant of ordinary crime, then the Executive is conducting a search and seizure that "violate[s] the Fourth Amendment in its intensity and scope."[185] In this way, the collection and use of such unrelated evidence under FISA is analogous to the general warrants and writs of assistance of the eighteenth century that the Fourth Amendment was specifically enacted to address. Like the general

183. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 19 (1968) ("The scope of a search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible." (citing Warden v. Hayden, 387 U.S. 294, 310 (1967) (Fortas, J., concurring))); Florida v. Jimeno, 500 U.S. 248, 251 (1991) ("The scope of a search is generally defined by its expressed object." (citing United States v. Ross, 456 U.S. 798 (1982))); Horton v. California, 496 U.S. 128, 140 (1990) ("If the scope of the search exceeds that permitted by the terms of a validly issued warrant or the character of the relevant exception from the warrant requirement, the subsequent seizure is unconstitutional without more."); Florida v. Royer, 460 U.S. 491, 500 (1983) ("The [Fourth] Amendment's protection is not diluted in those situations where it has been determined that legitimate law enforcement interests justify a warrantless search: the search must be limited in scope to that which is justified by the particular purposes served by the exception."); United States v. Ross, 456 U.S. 798, 823 (1982) ("The scope of a warrantless search based on probable cause is no narrower—and no broader—than the scope of a search authorized by a warrant supported by probable cause. Only the prior approval of the magistrate is waived; the search otherwise is as the magistrate could authorize."); Cupp v. Murphy, 412 U.S. 291, 295 (1973) ("[T]he scope of a warrantless search must be commensurate with the rationale that excepts the search from the warrant requirement."); *Warden*, 387 U.S. at 310 ("[W]e have refused to permit use of articles the seizure of which could not be strictly tied to and justified by the exigencies which excused the warrantless search.").

184. *See supra* Part I.C.5.

185. *Terry*, 392 U.S. at 18.

warrants of old that permitted limitless searches, "[t]he insidious, far-reaching and indiscriminate nature of electronic surveillance—and, most important, its capacity to choke off free human discourse that is the hallmark of an open society—makes it almost, although not quite, as destructive of liberty, as the 'kicked-in door.'"[186]

These principles go as far back as *Boyd v. United States*, the Court's first major interpretation of the Fourth Amendment.[187] In *Boyd*, the Court held that a person could not be compelled to produce his own papers to be used as evidence against himself in court.[188] Doing so would be a violation of the Fourth Amendment's prohibition on unreasonable searches and seizures,[189] even though there were no "circumstances of aggravation" on the government's part, such as breaking down doors or opening drawers without a warrant.[190] The Court stressed that "[i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is [in] the invasion of his indefeasible right of personal security, personal liberty and private property."[191]

Although the Court in *Boyd* tied the right of privacy to private property, the underlying principle was that unless the "papers or effects" or whatever else the government wanted to seize was contraband or instruments of a crime, they may not be reached by any warrant or seized by the police.[192] If they were seized, the government could not use them in evidence.[193] The Court noted that this was a reaction to the evils of the use of the general warrants in England and the writs of assistance in the Colonies, and was intended to protect against invasions of the "sanctity of a man's home and the privacies of his life" from searches under indiscriminate, general

186. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 388 (1974) (quoting Monroe v. Pape, 365 U.S. 167, 209 (1961) (Frankfurter, J, dissenting)).

187. David A. Sklansky, *The Fourth Amendment and Common Law*, 100 COLUM. L. REV. 1739, 1740 (2000). *See also* Olmstead v. United States, 277 U.S. 438, 474 (1928) (describing United States v. Boyd as the decision that "will be remembered as long as civil liberty lives in the United States").

188. Boyd v. United States, 116 U.S. 616, 630 (1886).

189. The Boyd Court also held that compelling a person to produce his papers would violate the Fifth Amendment's privilege against self-incrimination, but this aspect of the Court's holding is not discussed in this Note. *Id.* at 633.

190. *Id.* at 630.

191. *Id.*

192. *Id.* at 623–24.

193. *Id.*

authority.[194] The notion that police could only search and seize evidence that was contraband or instruments of a crime, and not "mere evidence," became known as the mere evidence rule.[195]

The mere evidence rule defined the legal scope of a search for the next four decades, until the Supreme Court overturned it in *Warden v. Hayden*.[196] In *Warden*, the Court rejected the distinction between the seizure of "mere evidence" (that is, items for evidentiary purposes only) and the seizure of items that were instrumentalities, fruits, or contraband.[197] The Court found that, on its face, the Fourth Amendment protected the "'right of the people to be secure in their persons, houses, papers, and effects . . .,' without regard to the *use* to which any of these things are applied."[198] The mere evidence rule failed to protect this "right of the people" because individual privacy could be infringed both by a search directed at "a purposely evidentiary object" and a search directed at an instrumentality or fruit of a crime, or contraband.[199] That is, the Fourth Amendment protects individual privacy whether the police conducted a search for "mere evidence" or for fruits or instrumentalities of a crime, or for contraband.[200]

In his concurrence, Justice Fortas lamented the majority's decision to strike down the mere evidence rule, which he saw as essential to enforce the Fourth Amendment's prohibition against

194. *Id.* at 625–27, 630.

195. The mere evidence rule was articulated in Gouled v. United States, 255 U.S. 298, 309 (1921). The Court stated that:

> [a]lthough search warrants have thus been used in many cases ever since the adoption of the Constitution, and although their use has been extended from time to time to meet new cases within the old rules, nevertheless it is clear that, at common law and as the result of the *Boyd* and *Weeks Cases* . . . they may not be used as a means of gaining access to a man's house or office and papers solely for the purpose of making search to secure evidence to be used against him in a criminal or penal proceeding, but that they may be resorted to only when a primary right to such search and seizure may be found in the interest which the public or the complainant may have in the property to be seized, or in the right to the possession of it, or when a valid exercise of the police power renders possession of the property by the accused unlawful and provides that it may be taken.

Id. (citing *Boyd*, 116 U.S. at 623–24).

196. Warden v. Hayden, 387 U.S. 294, 300–01 (1967).

197. *Id.* at 300.

198. *Id.* at 301 (emphasis added) (quoting U.S. CONST. amend. IV).

199. *Id.* at 301–02.

200. *Id.* at 306–07.

general searches—the amendment's very purpose.[201] In doing so, the majority had "needlessly destroy[ed], root and branch, a basic part of liberty's heritage."[202] In his dissent, Justice Douglas had harsher words for the majority. *Boyd*, according to Justice Douglas, not only established the requirements for a warrant, but also created a "zone of privacy which no government official may enter."[203] In striking down the mere evidence rule, the Court had also whittled away at the right that was at the very heart of the Fourth Amendment: the right of an individual to be free from warrantless, indiscriminate searches.[204] Justice Douglas pointed out that:

> [t]hose who wrote the Bill of Rights believed that every individual needs both to communicate with others and to keep his affairs to himself. That dual aspect of privacy means that the individual should have the freedom to select for himself the time and circumstances when he will share his secrets with others and decide the extent of that sharing. This is his prerogative, not the States'. The Framers . . . knew what police surveillance meant and how the practice of rummaging through one's personal effects could destroy freedom.[205]

Despite the death of the mere evidence rule, the Court has held in later cases that the Fourth Amendment prohibits "general searches."[206] A warrantless search must be particularized and specify exactly what must be seized, and it must be limited in scope to the reasons the search was initiated.

The amended FISA, however, stands this basic rule on its head. As mentioned above, the Executive may conduct FISA surveillance for the primary purpose of collecting evidence to use in a criminal prosecution, and may then share this information with law enforcement officials. Law enforcement officials may then charge persons—even third parties who were not originally targets of the FISA surveillance—with ordinary crimes. The extension of criminal charges to persons beyond the scope of the initial investigation is

201. *Id.* at 310–12 (Fortas, J., concurring).

202. *Id.* at 312.

203. *Id.* at 315 (Douglas, J., dissenting).

204. *Id.* at 325.

205. *Id.* at 323–24.

206. *See, e.g.*, Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 325 (1979) ("Nor does the Fourth Amendment countenance open-ended warrants, to be completed while a search is being conducted and items seized or after the seizure has been carried out.").

essentially a twenty-first century reincarnation of the general warrant and writ of assistance.[207] And like those historical procedures, today's procedures under FISA, as amended by the Patriot Act, violate the Fourth Amendment because they are indiscriminate.

The Court's history of condemning indiscriminate searches or seizures rests on the fact that such searches expose individuals to interferences by government when there is simply no good reason to do so.[208] Similarly, in the case of FISA surveillance, there is simply no good reason to avoid the Constitutional protections of Title III when the defendant will ultimately not be charged with a crime related to the reason for the FISA authorization in the first place. The concern about unjustified searches and seizures rests on the notion that every citizen is entitled to security of his person and property unless and until the government is able to provide an adequate justification.[209]

The second reason for the Court's condemnation of indiscriminate searches and seizures is that they are conducted at the discretion of the Executive, who may act "despotically and capriciously in the exercise of the power to search and seize."[210] The concern is that the Executive would search and seize arbitrarily.[211] Thus, the whole reason for constitutional safeguards is to "condemn[] the petty tyranny of unregulated rummagers."[212]

IV. The Solution

A. The Rebirth of the Mere Evidence Rule in FISA Cases

The solution proposed by this Note is for regular, non-secret Article III courts to suppress FISA-obtained evidence when introduced against a criminal defendant who has been charged solely with an ordinary crime—that is, a crime unrelated to a significant foreign intelligence purpose, the reason behind the FISA surveillance in the first place. This would constitute an initiation of a twenty-first century version of the mere evidence rule. Under this rule, any evidence that is unrelated to the purpose of the FISA authorization in the first place—foreign intelligence—constitutes "mere evidence" and

207. Amsterdam, *supra* note 186, at 411.
208. *Id.*
209. *Id.*
210. *Id.*
211. *Id.*
212. *Id.*

must be suppressed for the constitutional reason discussed above: the scope of the search and seizure is not commensurate with its purpose.

A mere evidence rule would deter the use of FISA for ordinary prosecution. "If the alleged 'end run' around the Fourth Amendment yields no usable evidence, then prosecutors would have little incentive to improperly rush toward FISA."[213] The rule would also alleviate the concern that the government may use FISA as a substitute for normal criminal law enforcement and Title III "based on trumped up evidence of a connection to a foreign threat" by removing all motivation for employing such a tactic in the first place.[214]

Furthermore, the rule would serve as a use limit that would function, after the fact, in the same way that the now-defunct primary purpose test functioned before the surveillance: by ensuring that FISA evidence would only be used against a defendant with credible ties to a foreign power and charged with the most serious national security offenses.[215] In working after the fact, the rule would avoid the problems that led to the breakdown of "the wall" in the first place: the sharing of information between intelligence agencies and law enforcement would still occur, but the latter's use of such evidence would be strictly limited. Although the rule does not completely alleviate the risk that the government will still invade the privacy of Americans, it would "diminish the Executive's ability to exploit that intrusion" because the government would not be able to use that evidence in court.[216]

B. Applying the Mere Evidence Rule

The idea of applying a mere evidence rule in FISA cases would not be completely novel. The Ninth Circuit, in an opinion by Chief Judge Kozinki, which was endorsed by nine out of eleven judges sitting en banc, recently applied a similar rule—albeit in a different context—to the same problem addressed in this Note. The case, *United States v. Comprehensive Drug Testing, Inc.*, dealt with the federal investigation into steroid use by professional baseball

213. Matthew R. Hall, *Constitutional Regulation of National Security Investigation: Minimizing the Use of Unrelated Evidence*, 41 WAKE FOREST L. REV. 61, 103 (2006).

214. *Id.*

215. *Id.*

216. *Id.*

players.[217] The Ninth Circuit used the case as an opportunity to create procedural safeguards that federal courts must follow when issuing search warrants for electronically stored information.[218]

In 2002, the FBI launched an investigation into the Bay Area Lab Cooperative ("BALCO") because it was suspected of providing steroids to professional baseball players.[219] At the same time, the Major League Baseball Players Association and Major League Baseball agreed to mandatory drug tests of all professional baseball players.[220] Administered by Comprehensive Drugs Testing ("CDT"), an independent corporation, the program required all Major League players to undergo urine tests for banned substances.[221] The results, which were confidential, were not to be used to convict or penalize any particular player who tested positive, but rather were to be assessed in the aggregate to determine whether more than five percent of the players were using banned substances; if so, additional testing in future seasons would be required.[222]

After learning that ten baseball players had tested positive for steroid use, the FBI obtained a subpoena from the Northern District of California for "*all* 'drug testing records and specimens'" of the baseball players in CDT's possession.[223] The baseball players and CDT moved to quash the subpoenas.[224] On the same day that the motion to quash was filed, the FBI obtained a warrant—this time from the Central District of California—that authorized a search of CDT's records.[225] The warrant, unlike the subpoena, contained an important limitation: it prohibited the government from searching the records of persons other than the ten baseball players for whom the FBI had probable cause to believe had taken banned substances.[226] In executing the warrant, however, the government searched and seized

217. United States v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2009 WL 2605378, at *1 (9th Cir. Aug. 26, 2009).

218. *Id.*

219. *Id.*

220. *Id.*

221. *Id.*

222. *Id.*

223. *Id.* (emphasis added).

224. *Id.*

225. *Id.*

226. *Id.*

the records not just of those ten players, but of hundreds of professional baseball players.[227]

The government's disregard for the narrow scope of the warrant, as well as its indiscriminate rummaging through electronic databases for evidence, is similar to the problem discussed in this Note: How should courts treat evidence of criminal activity that the government seizes pursuant to a warrant, when that criminal activity was not within the scope of the warrant? In *Comprehensive Drug Testing*, the government searched hundreds of electronic records in order to locate records of ten baseball players for whom it had probable cause to seize. But it also seized the records of hundreds of other people under the "plain view" doctrine.[228] The records, all contained in one electronic directory, contained a vast number of drug test results, not only of the ten players for whom the FBI had probable cause, but also of hundreds of professional baseballs players, other sports organizations, and a non-sporting entity.[229] Other than the bad luck of having their tests stored in the same computer as the ten baseball players named on the warrant, many of these third parties were completely unrelated.[230]

Similarly, FISA permits the government to search and seize—usually in the form of electronic surveillance—information unrelated to the purpose of the FISA warrant, as well as to obtain information about third parties not named as targets of surveillance in the FISA warrant. As long as the FBI is able to articulate a "significant" foreign intelligence purpose for the investigation at the very outset—based perhaps on only the slightest ties to a foreign power or its agent—the government may conduct surveillance not only on the FISA target, but also on any other third party unfortunate enough to share the target's trunk line: the line of communication between the communications carrier and a network of telephones, computers, and fax machines.[231] Thus, a FISA warrant issued for one person would require the review of a large number of electronic communications belonging to unrelated third parties, which the government could—using the same argument of plain view that it did in *Comprehensive*

227. *Id.*

228. *Id.* at *6.

229. *Id.* at *14.

230. *Id.* at *14.

231. Pollak, *supra* note 17, at 259–60.

Drug Testing—then use as evidence against defendants charged with ordinary crimes.

The government's main argument in *Comprehensive Drug Testing* is that law enforcement officials are justified in going beyond the scope of a warrant because of its inability to locate and seize the objects of the search without revealing the electronic files of others.[232] The government would likely make this same argument in response to complaints that FISA searches netted evidence and third parties well beyond the initial scope of the FISA warrant. According to the government, if evidence of crimes is discovered during the search, the evidence may be seized under the plain view doctrine.[233] Under the plain view doctrine, law enforcement officials may constitutionally seize evidence in plain view if, first, the seizing officer is lawfully located in a place from which the evidence can be seen; second, the seizing officer himself has a lawful right of access to evidence;[234] and third, the seizing officer has probable cause to believe that the evidence in plain view is incriminating in nature.[235] In *Comprehensive Drug Testing*, however, the Ninth Circuit found the government's conduct impermissible and explicitly rejected its plain view argument.[236]

Rejecting the government's argument about the plain view doctrine, the Ninth Circuit established guidelines to ensure that a search warrant for electronic data does not "become a vehicle for the government to gain access to data which it has no probable cause to collect."[237] Among those guidelines is a requirement that the government "forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data."[238] Should the government refuse to waive the use of the plain view doctrine, the "judge should order that the seizable

232. *Comprehensive Drug Testing, Inc.*, 2009 WL 2605378, at *3-4.

233. *Id.* at *6.

234. New York v. Class, 475 U.S. 106, 118–19 (1986).

235. Arizona v. Hicks, 480 U.S. 321, 324 (1987). *See also* Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971) (finding that "the extension of the original justification [for the search] is legitimate only where it is immediately apparent to the police that they have evidence before them; the 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges").

236. *Comprehensive Drug Testing, Inc.*, 2009 WL 2605378, at *6–7.

237. *Id.* at *15.

238. *Id.* at *7.

and non-seizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether."[239] Furthermore, the government must destroy or return any data that does not fall within the scope of the warrant to the party from whom the government obtained it.[240]

The Ninth Circuit's en banc opinion suggests that the government's justification of "plain view" may be unworkable not only in the context of a search of electronic records, but also in the context of FISA surveillance. The Ninth Circuit's guidelines would have the same effect when applied to criminal cases as the mere evidence rule advocated in this Note: the government would not be permitted to use in court any evidence that is unrelated to the original scope of the warrant.

The mere evidence rule, if applied to FISA cases, would restore the judiciary to its rightful role as the enforcer of the Fourth Amendment by allowing federal judges to limit and regulate Executive surveillance. For example, a defendant challenging the admission of FISA evidence may be successful if the judge determines that the crime has only a weak connection to the foreign intelligence purpose specified in the FISA order. Thus, evidence that the defendant trafficked drugs for own profit, rather than channeling the proceeds to fund a terrorist organization, would constitute "mere evidence" and would be excluded. Under this rule, however, the actual narcotics—if found pursuant to the FISA warrant—could be rightfully seized as contraband, but could not be used against the defendant charged solely with narcotics trafficking.

Conclusion

The amended FISA increases the risk that the government will use new technologies to intrude into the lives of citizens to an unprecedented degree. The guarantee against unreasonable searches and seizures "was written and should be read to assure that any and every form of such interference is at least regulated by fundamental law so that it may be 'restrained within proper bounds.'"[241] In order to keep us from sliding back to a time when the abuse of individual privacy under general warrants was the norm, courts must prohibit

239. *Id.*

240. *Id.* at *9.

241. Amsterdam, *supra* note 186, at 400 (citation omitted).

the use of FISA fruits in criminal prosecutions that have no relation to the reason for the interference in the first place.