University of Michigan Journal of Law Reform

Volume 42

2008

Shu'ubiyya or Security? Preserving Civil Liberties by Limiting FISA Evidence to National Security Prosecutions

William Pollak
University of Michigan Law School

SHU'UBIYYA† OR SECURITY? PRESERVING CIVIL LIBERTIES BY LIMITING FISA EVIDENCE TO NATIONAL SECURITY PROSECUTIONS

William Pollak*

Ever since 9/11, this Administration has put forward a false choice between the liberties we cherish and the security we demand.

—Barack Obama
commenting on the
FISA Amendments Act of 2008[1]

INTRODUCTION

In the immediate aftermath of September 11, 2001, Congress rushed to eliminate many of the legal restrictions on intelligence gathering that were blamed for allowing the 9/11 attacks to go undetected. The Foreign Intelligence Surveillance Act ("FISA"), enacted in 1978, was one key statute targeted for reform. Prior to 9/11, FISA enabled the government to conduct foreign surveillance without demonstrating probable cause of criminal activity[2] but restricted the use, in a criminal prosecution, of information gathered during a foreign intelligence investigation.[3] The USA

† Shu'ubiyya loosely translates to anti-Arabism or discrimination against Arabs. It is a word with a deep history. Initially, shu'ubiyya did not have a derogatory connotation and was used interchangeably with taswiya (equality) to convey a sense of the Persians struggle for equality with Arabs. In modern times, however, shu'ubiyya has emerged in the political lexicon with purely derogatory connotations.

* University of Michigan Law School, J.D. 2008; Princeton University A.B. 2003. Thanks to Professor Scott Hershovitz for helping me develop my ideas and for providing useful comments on a draft of this Note.

1. Jane Hamsher, *Barack Obama Statement on FISA*, Jan. 28, 2008, http://firedoglake.com/2008/01/28/barack-obama-statement-on-fisa/; Patrick Casey, *Putting Obama and the Dems on the Defensive*, AMERICAN THINKER, June 20, 2008, http://www.freerepublic.com/focus/f-news/2034053/posts; FISAlist: Barack, Jan 2008 On FISA, http://my.barackobama.com/page/community/post/92104/gGxlHh (Jul. 6, 2008, 2:24 EST).

2. The current version of FISA only requires the government to demonstrate probable cause 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) (2000). In addition, FISA does not include an exclusionary rule and it only provides for limited judicial review of government applications. *See infra* text accompanying notes 20–26.

3. The pre-USA PATRIOT ACT version of FISA required the government to demonstrate that the collection of foreign intelligence information was the primary purpose of the FISA warrant. This restriction limited the use of FISA evidence in ordinary criminal prosecutions. *See* discussion *infra* Part II.

PATRIOT ACT, however, amended FISA and eliminated these restrictions.[4] Under the Patriot Act, enacted on October 26, 2001, the government now may obtain a FISA warrant to wiretap[5] a suspect solely on the basis of an unchallenged certification by the government that the suspect may be the agent of a foreign power or terrorist organization. In addition, the amended act allows any information gathered pursuant to a FISA warrant to be used in an "ordinary criminal prosecution."[6]

As a result of these changes, the government can access the private information of a broad swath of people who have only minimal ties to foreign organizations. Any evidence, gathered pursuant to these wiretaps, is admissible in a criminal trial even if the surveillance reveals that, in fact, the suspect has no ties to any foreign power or terrorist organization.[7] As a result, FISA may lower the statutory restrictions on the gathering of evidence, particularly in criminal prosecutions of Muslim Americans and recent immigrants, who could easily be characterized as agents of foreign powers simply because they continue to associate with their native countries.[8]

Equally disturbing, the admission of FISA evidence in non-foreign intelligence prosecutions may result in the arbitrary enforcement of the criminal laws. Surveillance of a FISA subject often necessitates monitoring all calls and emails from the suspect's home and office including those of innocent family members or co-workers. Indeed, internet surveillance of a FISA suspect often requires capturing and reading the internet traffic of all the people

4. USA PATRIOT ACT, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter the Patriot Act].

5. FISA not only allows the government to listen to a suspect's phone calls, but also allows the government to read a suspect's emails, to conduct "sneak-and-peak" searches of a suspect's residence, and to use GPS technology to track a suspect's movements. *See infra* notes 81, 126, 128.

6. I use the term "ordinary criminal prosecutions," and later, "ordinary crimes," to refer to those criminal prosecutions and crimes without any connection to national security.

7. The Immigration and Nationality Act, § 219(a)(8), 8 U.S.C. § 1189(a)(1)-(8) (2006), sets out a scheme for the Secretary of State to designate certain organizations as "foreign terrorist organization[s]." To make the designation, the Secretary has to make specific findings that "the organization is a foreign organization"; that "the organization engages in terrorist activity (as defined in section 1182(a)(3)(B))"; and that "the terrorist activity of the organization threatens the security of United States nationals or the national security of the United States." § 1189(a)(1); *see also* 18 U.S.C.A. § 2339B (2006) making it a crime to provide "material support" to a foreign terrorist organization.

8. *See generally* Eric Lichtblau, *Thousands From Muslim Nations Were Investigated Before '04 Election, Data Show*, N.Y. TIMES, Oct. 31, 2008, at A17, *available at* http://www.nytimes.com/2008/10/31/us/31inquire.html (presenting evidence that "more than 2,500 foreigners [seventy-nine percent of whom were from Muslim countries] in the United States were sought as 'priority leads' in the fall of 2004 because of suspicions that they could present threats to national security," the vast majority of whom were interrogated and detained but never charged).

who live in the suspect's building or work in the suspect's office. Any evidence of criminal activity conducted by other persons unfortunate enough to live or work in the vicinity of a FISA suspect may also be captured and admitted in a criminal trial for an ordinary crime.

At the same time, persuasive arguments can be made for a lower standard to allow for the electronic surveillance of terrorists and the acquisition of foreign intelligence information. Foreign intelligence collection tends to be programmatic, focusing on nascent schemes and following up on ambiguous leads.[9] In addition, terrorists operating in a loosely connected cell structure are hard to identify and are typically well-trained in avoiding detection. Finally, the desire for secrecy and the devastating cost of failing to detect a terrorist plot necessitate an expedient approval process and may call for a decreased standard of judicial review in cases involving national security.

This Note attempts to balance these concerns by proposing a rule limiting the admission of evidence gathered under FISA to cases involving foreign intelligence/national security crimes such as terrorism, sabotage, and espionage, and cases involving crimes "inextricably intertwined" with national security offenses. Under this test, for FISA evidence to be admissible, (1) the defendant must be indicted and charged with a national security crime or a crime involving the "material support" of a terrorist organization or a foreign government; and (2) the judge must find, after an *in camera* review, that the government has demonstrated a link between a foreign intelligence crime and the prosecution at issue. Evidence obtained under a FISA warrant would be excluded from prosecutions of ordinary crimes without a sufficient nexus to national security.

Part I of this Note addresses the restrictions on intelligence gathering under FISA prior to 9/11 and the motivations underlying the Patriot Act's revisions to FISA. Part II discusses the problems with the "primary purpose" test, which was in effect prior to the Patriot Act's revisions to FISA. Part III reviews the various policy and constitutional arguments made against the Patriot Act's "significant purpose" test. Part IV proposes that Congress enact a new "inextricably intertwined" test to govern the admission of FISA material in criminal prosecutions. Specifically, this Part looks at sixty criminal cases in which FISA material was admitted and evaluates how the "inextricably intertwined" test would play out in those

9. William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1152–53 (2003) [hereinafter Banks, *Secret Surveillance*].

cases. Part V examines the arguments in favor of the inextricably intertwined test. Finally, Part VI counters the argument that the inextricably intertwined test violates the plain view doctrine.

I. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT ("FISA")

Under the pre-Patriot Act version of FISA, a high ranking member of the executive branch applying for a surveillance order from the secret FISA court[10] had to certify that: (1) the information sought was foreign intelligence information;[11] (2) "the purpose"[12] of the surveillance was to obtain foreign intelligence information; and (3) such information could not reasonably be obtained by normal investigative techniques.[13] The applicant also had to identify the target of the surveillance, if known, and make a preliminary showing that the target of the electronic surveillance was a "foreign power,"[14] or an "agent of a foreign

10. FISA established a special court, the Foreign Intelligence Surveillance Court ("FISC"), that meets in secret, *ex parte* proceedings. 50 U.S.C. § 1803(a) (2000).

11. 50 U.S.C. § 1804(a)(7)(A) (2000).

12. This provision was amended by the USA PATRIOT ACT, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (2001) (amending 50 U.S.C. §§ 1804(a)(7)(B), 1823 (a)(7)(B) (2000)), to read: "*a significant* purpose of the surveillance is the collection of foreign intelligence" (emphasis added). *See infra* Part III.

13. 50 U.S.C. § 1804(a)(7)(C) (2000); *see also id.* § 1805(a)(3).

14. *Id.* § 1801(a). Under FISA, a "foreign power" includes:

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

Id.

power."[15] In addition, prior to the Patriot Act the government had to specify, in the application, the places where the surveillance was to be directed.[16]

---

15. 50 U.S.C. § 1801(b) (2000) defines an "agent of a foreign power" as:

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(C) engages in international terrorism or activities in preparation therefore; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefore, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

16. The Patriot Act amended FISA to allow "roving wiretaps" which enable the surveillance to follow the suspect as he switches phones. For a description of this change, see Jeremy C. Smith, Comment, *The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security*, 82 N.C. L. REV. 412, 416–23 (2003). It should be noted that roving wiretaps were first authorized by some circuits in the early 1990s. *See, e.g.*, United States v. Bianco, 998 F.2d 1112, 1124 (2d Cir. 1993) (interpreting 18 U.S.C. § 2518(11)(a) (2006) as authorizing a "roving wiretap" so long as surveillance was limited to communications involving the identified speaker and relating to specific crimes the speaker was suspected of participating in), *cert. denied*, 114 S. Ct. 1644 (1994); United States v. Petti, 973 F.2d 1441, 1445 (9th Cir. 1992), *cert. denied*, 113 S. Ct. 1859 (1993).

The protections afforded a person under FISA depart substantially from those under Title III[17] in the following ways: (1) FISA does not require a showing of probable cause of criminal activity; (2) FISA only provides for limited judicial review; (3) FISA lacks an exclusionary rule; (4) FISA provides for a significantly longer period of surveillance; and (5) FISA does not provide notice to the person under surveillance or give the defendant an adequate opportunity to challenge the certifications underlying the FISA application.

First, the most important of these differences is the lack of probable cause requirement for a FISA warrant. Title III only authorizes electronic surveillance if the court determines, based on the sworn testimony of a government agent, that there is probable cause that an individual is committing, has committed, or is about to commit a particular offense.[18] FISA, by contrast, only requires a high-ranking government official to certify that the target of the surveillance acts on behalf of a foreign power, engages in clandestine intelligence activities, or participates in international terrorism or sabotage.[19] Significantly, the probable cause requirement under Title III acts as a large hurdle that prevents the government from pretextually utilizing wiretaps to target specific groups for whom the government lacks reasonable suspicion of criminal activity.

Second, due in part to the lack of a probable cause requirement, FISA applications are subjected to a significantly lower level of judicial scrutiny than Title III applications.[20] The FISC will only

17. The Federal Wiretap Act (Title III), 18 U.S.C. § 2510 (2000), was adopted in 1968 and expanded in 1986. It establishes procedures for government surveillance of voice, email, fax, and Internet communications. *Id.* Under Title III, the government must obtain a court order issued by a federal district judge who must conclude, based on an affidavit submitted by the government, that there is probable cause to believe that a crime has been, is being, or is about to be committed. *Id.*

18. 18 U.S.C. § 2518(3)(a) (2006). Title III also requires the applicant to have exhausted all other investigatory techniques before seeking a warrant, § 2518(3)(c), an important requirement which is absent from FISA. This is a significant difference because the exhaustion prerequisite obligates a Title III applicant to pursue electronic surveillance only as a last resort when other investigatory techniques have failed. *See* 18 U.S.C. § 2518(1)(c) (2006) (requiring a judicial determination that "normal investigative procedures have failed or reasonably appear to succeed if tried or to be too dangerous").

19. 50 U.S.C.A. § 1802(a)(1) (2000); 50 U.S.C. § 1805(a)(1) (2000); 50 U.S.C.A. § 1804(a)(3) (2000).

20. If the target of the surveillance is a U.S. person, a term that includes U.S. citizens and permanent residents, the FISC judge must find that the certifications submitted by the government are not clearly erroneous, and that proper procedures are followed to minimize the intrusion on the target's privacy and to eliminate information that is not pertinent. 50 U.S.C. § 1805(a)(5) (2000); 50 U.S.C. § 1801(h) (2000); *see also* United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984) (stating that the government's certification "is, under FISA, subjected to only minimal scrutiny by the courts"); H.R. REP. No. 95-1283, at 80 (1978) (ex-

scrutinize the government's application if the target is a U.S. citizen and, even in cases involving U.S. citizens, the court will only review the government's certifications for clear error.[21] The clear error standard is so deferential that it has been interpreted to prevent the FISC judges from second guessing the government's assertions.[22] The FISC judge's role, therefore, is only to evaluate whether the application facially complies with the statutory requirements.[23] Moreover, when a defendant challenges the admission of FISA evidence at his trial, the district court judge is similarly constrained in his review and limited to evaluating "procedural regularity."[24]

Third, courts have consistently declined to exclude unlawfully seized FISA evidence[25] and, as a result, there is little to deter the applicant from making unsupported or inaccurate assertions. Even in cases in which, after the investigation concludes, falsehoods have been discovered in FISA applications, the evidence obtained from the surveillance has been deemed admissible.[26]

---

plaining that the "clearly erroneous standard of review is not, of course, comparable to a probable cause finding by the judge").

21. 50 U.S.C. § 1805(a)(5) (2000).

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

23. *Id.*

24. H.R. REP. No. 95-1283, pt. I, at 92–93 (1978) ("[I]n determining the legality of a surveillance . . . the trial judge . . . [is] not to make determinations which the issuing judge is not authorized to make. Where the bill specifies the scope or nature of judicial review in the consideration of an application, any review under these subsections is similarly constrained. For example, when reviewing the certifications required by [50 U.S.C. § 1804(a)(7) (2000)], unless there is a prima facie showing of a fraudulent statement by a certifying officer, procedural regularity is the only determination to be made if a non-U.S. person is the target . . . ."), *cited in Duggan*, 743 F.2d at 77; United States v. Badia, 827 F.2d 1458, 1463 (11th Cir. 1987).

25. 50 U.S.C. § 1806(g) (2000) (containing FISA's exclusionary rule). *But see* United States v. Ajlouny, 629 F.2d 830, 839–40 (2d Cir. 1980) (finding that, because the exclusionary rule did not apply in the case, any evidence obtained via unlawful surveillance would not be suppressed); 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) (admitting the FISA evidence even though the government failed to obtain the proper authorization from the Attorney General until eight months into the surveillance); United States v. Marzook, 435 F. Supp. 2d 778, 788–91 (N.D. Ill. 2006) (declining to apply the exclusionary rule to evidence obtained in a physical search of the defendant's house which was unauthorized under the 1993 version of FISA).

26. *See infra* notes 66–67; *see also* United States v. Holy Land Found. for Relief and Dev., No. 3:04-CR-240-G, 2007 WL 2011319, at *3 (N.D. Tex. Jul. 11, 2007) (declining to apply the exclusionary rule to evidence obtained pursuant to a FISA application which contained several errors); United States v. Daly, Nos. 05-10718, 05-10719, 05-10728, 05-10729, 2007 WL 2212362, at *1 (9th Cir. Aug. 2, 2007) (holding that "[e]ven if the statements that Jamal 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").

Fourth, while the data collection period is limited to thirty days under Title III,[27] FISA surveillance may be authorized for up to one hundred and twenty days.[28] FISA also contains a provision authorizing the Attorney General, in emergency situations, to begin surveillance without a FISC order, so long as he receives FISC approval within seven days of the initiation of the surveillance.[29]

Finally, under Title III, targets must be provided notice within ninety days of the termination of the surveillance[30] and under the Federal Rules of Criminal Procedure ("FRCP"), surveillance targets must be given immediate notice of an ordinary search warrant.[31] Under FISA, however, targets are only provided notice of the surveillance if the transcripts are admitted in a criminal proceeding.[32] More importantly, when challenging the admissibility of FISA evidence in the subsequent criminal trial, the defendant will be denied access to the background materials that supported the FISC order—the application, affidavits, surveillance logs, or statements from informants—and therefore will often be unable to mount an effective defense.[33] Indeed, over the thirty-year history of FISA no defendant has successfully challenged a FISA application, in large part because no court has ordered the disclosure of a FISA applica-

27. 18 U.S.C. § 2518(5) (2006).

28. 50 U.S.C. § 1805(e)(1) (2000). The Patriot Act extended the permissible surveillance time period to up to one year when targeting a foreign power, and up to 120 days when targeting the agent of a foreign power. *Id.* After the first one hundred and twenty days, the surveillance is frequently renewed without amending or altering the original application. In addition, the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 extended this period to one year when targeting persons reasonably located outside of the United States. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 701(g)(1)(B), 122 Stat. 2436, 2440 (2008).

29. 50 U.S.C. § 1805(f) (2000) (allowing the Attorney General 72 hours to seek FISC approval after the initiation of the surveillance). This period was extended from seventy-two hours to seven days by the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008. H.R. 6304, 110th Cong. § 701(g)(1)(B) (2008).

30. 18 U.S.C. § 2518(8)(d) (2006).

31. FED. R. CRIM. P. 41(f)(1).

32. 50 U.S.C. §§ 1802(a)(3), 1806(f)–(g) (2000). FISC does not publish its decisions, its orders are sealed, and proceedings are ex parte. *See id.* § 1806(f).

33. *Id.* §§ 1806(f), 1825(g) (a reviewing court reviews these materials *ex parte* and *in camera* and discloses them to the defendant "only where disclosure is necessary to make an accurate determination of the legality of the [surveillance or physical search]"); *see also* United States v. Belfield, 692 F.2d 141, 148 (D.C. Cir. 1982) (acknowledging the difficult situation faced by a defense counsel attempting to challenge the admissibility of FISA materials: "They must argue that the determination of legality is so complex that an adversary hearing with full access to relevant materials is necessary. But without access to the relevant materials: their claim of complexity can be given no concreteness. It is pure assertion."); United States v. Holy Land Found. For Relief and Dev., No. 3:04-CR-240-G, 2007 WL 2011319, at *3–5 (N.D. Tex. Jul. 11, 2007) (denying Defendant's motion); United States v. Mubayyid, No. 05-40026-FDS, 2007 WL 3287393, at *2–3 (D. Mass. Nov. 5, 2007).

tion to the defendant.[34] Finally, if the FISA transcripts are not admitted at trial, the government is under no obligation to search through its surveillance records for exculpatory material, which deprives innocent defendants of any potential benefit from the surveillance.[35]

Congress approved these departures from Title III because it intended FISA to provide a practical mechanism for the executive branch to surveil agents of foreign powers, not to provide information for ordinary criminal investigations.[36] At the same time, the drafters of FISA recognized that intelligence gathering and law enforcement would overlap in the context of crimes such as terrorism, sabotage, and espionage.[37] As a result, several courts have interpreted § 1804(a) of FISA[38] as adopting a "primary purpose" test[39] which requires the executive to prove that the primary

34. *See In re* Grand Jury Proceedings, 347 F.3d 197, 203 (7th Cir. 2003) (finding that, as of September 14, 1988, "every FISA wiretap review had been conducted *in camera* and *ex parte*" and that there have been "no cases since that time where the review was conducted in any other fashion"); United States v. Sattar, No. 02 Cr. 395, 2003 U.S. Dist. LEXIS 16164, at *19–20 (S.D.N.Y. Sept. 15, 2003) (collecting cases finding that no court has ever ordered disclosure of the FISA application materials); United States v. Nicholson, 955 F. Supp. 588, 592 (E.D. Va. 1997) ("[T]his Court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance. To the contrary, every court examining FISA-obtained evidence has conducted its review *in camera* and *ex parte*."); *see also* Joshua L. Dratel, *Sword or Shield? The Government's Selective Use of its Declassification Authority for Tactical Advantage in Criminal Prosecutions*, 5 CARDOZO PUB. L. POL'Y & ETHICS J. 171 (2006) (arguing that the government's power to selectively declassify inculpatory evidence for use at trial, while, at the same time, denying the defense access to "classified" exculpatory evidence violates the Fifth and Sixth Amendments and proposing that FISA and the Classified Information Procedures Act be amended to put the government and the defense on equal footing with regard to classified information).

35. United States v. Marcos, No. SSSS 87 CR. 598(JFK), 1990 WL 16161, at *4 (S.D.N.Y. Feb. 15, 1990) (holding that the government is not required to turn over its surveillance records to the defendant or sift through its surveillance for exculpatory evidence if it does not intend to admit any surveillance evidence at trial).

36. *See* S. REP. No. 95-604, pt. 1, at 176 (1977) ("S. 1566 provides four limited situations in which natural persons may be made the target of an electronic surveillance without a probable cause showing of criminal activity."); H.R. REP. No. 95-1283, at 36 (1978) (explaining that FISA surveillances "are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information, which when it concerns United States persons must be necessary to important national concerns"); *see also* Banks, *Secret Surveillance*, *supra* note 9, at 1160 (discussing the placement of FISA in Title 50, War and National Defense, as demonstrating congressional intent, and noting that "Congress did not intend for FISA to in any way authorize surveillance for law enforcement purposes").

37. Banks, *Secret Surveillance*, *supra* note 9, at 1151–53.

38. 50 U.S.C. § 1804(a)(7)(B) (2000) requires the executive branch official to certify that the "purpose of the surveillance is to obtain foreign intelligence information."

39. The primary purpose test originated in United States v. Truong, 629 F.2d 908, 913–17 (4th Cir. 1980). *Truong* involved surveillance conducted prior to the passage of FISA but the decision was handed down after the passage of FISA. *Id.* at 914 n.4. It became an important guidepost in the subsequent judicial, executive and legislative interpretation of FISA. In *Truong*, the Fourth Circuit determined that there was an exception to the warrant

purpose of the surveillance is the collection of foreign intelligence, not the collection of evidence for use in a criminal prosecution.

In response to a number of court decisions applying the *Truong* primary purpose test, the Justice Department created the Office of Intelligence Policy and Review ("OIPR") to ensure institutional responsibility for FISA compliance.[40] From 1982 until 1995, OIPR operated without written guidelines for law enforcement personnel and consequently, "prosecutors had informal arrangements for obtaining information gathered in the FISA process."[41] These back-channel communications became quite common, to the point where prosecutors were often directing the surveillance.[42]

In one high-profile case, the Aldrich Ames espionage prosecution, OIPR advised the Attorney General that the results of the surveillance could be jeopardized by the close contact between law enforcement and intelligence personnel.[43] As a result, in 1995 Attorney General Janet Reno laid out a series of procedures to be followed with respect to national security wiretaps.[44]

Under the procedures laid out in the 1995 memo, the Criminal Division of the Justice Department could provide the FBI with advice regarding a foreign intelligence investigation so long as it did not inadvertently result in "either the fact or the appearance of the

---

requirement for national security investigations but that this exception only applied so long as the investigation's purpose was the collection of foreign intelligence. *Id.* at 915. Consequently, the Court determined that any evidence obtained after the investigation became primarily focused on criminal prosecution should be excluded. *Id.* at 915–16.

40. *See also* William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1234 (2007) [hereinafter Banks, *Death of FISA*]. In 2008, the OIPR came under the umbrella of the Justice Department's National Security Division and was renamed the "Office of Intelligence," materials available at http://www.usdoj.gov/nsd/intelligence/intelligence.htm.

41. *See id.* at 1234–40 (citing Diane Carraway Piette & Jessely Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall,"* 17 STAN. L. & POL'Y REV. 437, 448 (2006)).

42. OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS 24 (2004) [hereinafter 2004 OIG REPORT], *available at* http://www.usdoj.gov/oig/special/0506/final.pdf.

43. *See* Banks, *Secret Surveillance*, *supra* note 9, at 1162; *see also* Banks, *The Death of FISA*, *supra* note 40, at 1236 (citing NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 78 (2004) [hereinafter 9/11 COMMISSION REPORT]).

44. Memorandum from the Attorney General, Procedures for Contacts Between the FBI and Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations (Jul. 19, 1995) [hereinafter 1995 Procedures], *available at* http://www.fas.org/irp/agency/doj/fisa/1995procs.html. This Memorandum was based on recommendations from Deputy Attorney General, Jamie S. Gorelick, to Mary Jo White, Louis Freeh, Richard Scruggs, and Jo Ann Harris in March 1995. Memorandum from Jamie S. Gorelick, Deputy Attorney General, to Mary Jo White, Louis Freeh, Richard Scruggs, and Jo Ann Harris, http://www.usdoj.gov/ag/testimony/2004/1995_gorelick_memo.pdf (last visited Nov. 8, 2008).

Criminal Division directing or controlling an investigation."[45] In addition, under no circumstances could the Criminal Division instruct the FBI "on the operation, continuation, or expansion of FISA electronic surveillance."[46] These limitations were designed to ensure that the government only utilized the lower standards of FISA in cases involving threats to national security. Unfortunately, these guidelines were strictly interpreted by OIPR lawyers to the point where only a very limited amount of information was shared and a wall was created between the divisions of the Justice Department.[47]

II. PROBLEMS WITH THE PRIMARY PURPOSE TEST

The primary purpose test was a well-intentioned attempt to achieve a difficult balance between the seemingly incongruous policy objectives of providing the government with a lower threshold for surveillance of national security targets while protecting individual privacy rights.[48] The primary purpose test, however, failed on both accounts. Specifically, the wall that developed between the Criminal Division and intelligence personnel prevented the sharing of information and hindered valuable cooperation between the two branches without providing meaningful protection for individual rights.

According to the July 2001 General Accounting Office ("GAO") report, friction developed within the Justice Department during the 1990s because intelligence officials increasingly neglected to

45. 1995 Procedures, *supra* note 44, at ¶ A6.

46. *Id.*

47. *See* GENERAL ACCOUNTING OFFICE, COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED, GAO-01-780, 14 (2001), *available at* http://www.gao.gov/new.items/d01780.pdf; 2004 OIG REPORT, *supra* note 42, at 26; THE 9/11 COMMISSION REPORT, *supra* note 43, at 539 n.83.

48. *See* United States v. Truong, 629 F.2d 908, 915 (4th Cir. 1980) (affirming the district court's adoption of the primary purpose test because "once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution."); United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) (holding that, when a judge determines that foreign intelligence gathering is the "primary purpose" of a particular search and that "the accumulation of evidence of criminal activity [from that search] was incidental," an exception to the warrant requirement exists for the foreign intelligence gathering because "the need for electronic surveillance often cannot be anticipated in advance" and the public interest in foreign intelligence cases is greater than normal criminal cases); Zweibon v. Mitchell, 516 F.2d 594, 656–57 (D.C. Cir. 1975) (rejecting the government's argument that warrantless surveillance of a domestic organization [the Jewish Defense League] could be reasonable solely because "some information relevant . . . to foreign affairs [was] likely to be obtained from the surveillance").

share information with the Criminal Division under the mistaken belief that providing such information to law enforcement personnel would cause the FISC to reject applications to renew electronic surveillance of national security targets.[49] Intelligence officials fundamentally misunderstood the primary purpose test to mean exclusive purpose[50] and consequently shared almost no information with criminal prosecutors. On the other side of the wall, a desire to preserve the option of prosecution caused law enforcement officials to avoid any communication in those cases in which cooperation was the most crucial—cases in which evidence of foreign intelligence crimes had already been generated.[51] Moreover, the "wall" between criminal and intelligence investigations apparently "caused agents [in both divisions] to be less aggressive than they might otherwise have been in pursuing [FISA] surveillance powers in counterterrorism investigations."[52]

After 9/11, the Bush administration and many commentators blamed the failure to detect the terrorist plot on the FISA wall.[53] For example, in the joint hearings investigating the September 11th hijackings, a New York FBI agent testified that "the Wall's" restrictions prevented the FBI from obtaining information from the intelligence community regarding Khalid Al-Mihdar and Nawaf Al-Hazmi (who later turned out to be two of the September 11th hijackers).[54] The most prominent intelligence failure blamed on the FISA wall was the inability of FBI investigators to obtain a war-

49. GENERAL ACCOUNTING OFFICE, *supra* note 47, at 14.

50. *Id.*

51. *Id.*

52. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, STAFF STATEMENT NO. 9: LAW ENFORCEMENT, COUNTERTERRORISM, AND INTELLIGENCE COLLECTION IN THE UNITED STATES PRIOR TO 9/11 7 (2004), *available at* http://www.9-11commission.gov/staff_statements/staff_statement_9.pdf.

53. Jennifer L. Sullivan, *From "The Purpose" to "A Significant Purpose": Assessing the Constitutionality of the Foreign Intelligence Surveillance Act Under the Fourth Amendment*, 19 NOTRE DAME J.L. ETHICS & PUB. POL'Y 379, 397 (2005) [hereinafter Sullivan] (arguing that the failure to obtain a FISA warrant on Moussaoui and his computer stemmed from the failure to disseminate the "Phoenix Memo" to other FBI branches and "arguably [was] a major reason for the inability of law enforcement to detect and prevent the September 11th terrorist attacks"); *see also In re* Sealed Case, 310 F.3d 717, 747 n.29 (FISA Ct. Rev. 2002) (recounting the testimony of a senior FBI agent who argued that "the biggest threat to us now, [Usama Bin Laden], is getting the most 'protection.'").

54. *See* Jessica M. Bungard, *The Fine Line Between Security and Liberty: The Secret Court Struggle to Determine the Path of Foreign Intelligence Surveillance in the Wake of September 11th*, 7 U. PITT. J. TECH. L. & POL'Y, Spring 2004, at 1, 13, n.54 (2004) [hereinafter Bungard] (citing Prepared Statement of a New York Special Agent Before the United States Senate and the House of Representatives (Sept. 20, 2002), *available at* http://www.fas.org/irp/congress/2002_hr/092002fbi.html).

rant to search Zacarias Moussaoui's[55] computer when they detained him in Minneapolis for overstaying his tourist visa.[56] FBI "Headquarters also prohibited the field agents from notifying the Headquarters Criminal Division, fearing that any interest expressed in a criminal warrant and prosecution could jeopardize the chances of obtaining a FISA order."[57] Yet, at the same time, FBI headquarters did not pursue a FISA warrant because it believed it lacked sufficient evidence demonstrating that Moussaoui was an agent of a foreign power.[58] As a result, Moussaoui's computer was never searched and the terrorist plot never discovered. Therefore, it should come as no surprise that one commentator argued that: "[e]very major recent review of U.S. intelligence policy and organization [since 9/11] has called for increased information sharing, unity of command and control, and removal of barriers to joint and complementary action among U.S. government departments and agencies."[59] While these criticisms of FISA were certainly

55. Moussaoui is alleged to have been the "20th hijacker," one of the alleged masterminds behind the September 11th attacks. During his trial, Moussaoui repeatedly stated that he was not involved in the September 11 attacks, but that he was planning an attack of his own.

56. Banks, *Secret Surveillance*, *supra* note 9, at 1164–65; *see also* Memorandum from Coleen Rowley, Agent of the FBI, to Robert S. Mueller, Director of the FBI, (May 21, 2002), *available at* http://www.time.com/time/covers/1101020603/memo.html; Jerry Markon & Timothy Dwyer, *FBI Was Warned About Moussaoui; Agent Tells Court Of Repeated Efforts Before 9/11 Attacks*, WASH. POST, Mar. 21, 2006, at A01; Peggy Noonan, *Weenies or Moles: Did the FBI bungle the Moussaoui investigation—or worse?*, WALL ST. J., May 31, 2002, http://www.opinionjournal.com/columnists/pnoonan/?id=110001778; Heather MacDonald, *Why the FBI Didn't Stop 9/11*, CITY J., Autumn 2002, at 14, *available at* http://www.city-journal.org/html/12_4_why_the_fbi.html; Gary Schmitt, *Constitutional Spying: The Solution to the FISA Problem*, THE WKLY. STANDARD, Jan. 2–Jan. 9, 2006, at 11, 11, *available at* http://www.weeklystandard.com/Content/Public/Articles/000/000/006/533bcrdq.asp; William Kristol & Gary Schmitt, *Vital Presidential Power*, WASH. POST, Dec. 20, 2005, at A31, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121901027.html. *But see* Coleen Rowley, *FISA Not to Blame for Moussaoui Mess*, THE HUFFINGTON POST, Jan. 5, 2006, http://www.huffingtonpost.com/coleen-rowley/fisa-not-to-blame-for-mou_b_13310.html (disputing that FISA safeguards were to blame for the FBI's failure to obtain a search warrant for Moussaoui's computer).

57. Banks, *Secret Surveillance*, *supra* note 9, at 1164; *see also* REPORT OF THE JOINT INQUIRY INTO THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, S. REP. NO. 107-351, at xiii, 318–24 (2002), *available at* http://www.gpoaccess.gov/serialset/creports/pdf/fullreport_errata.pdf (discussing the mistaken view of agents involved in the Moussaoui investigation regarding the showing necessary to obtain a FISA warrant).

58. Banks, *Secret Surveillance*, *supra* note 9, at 1165.

59. Fred F. Manget, *Intelligence and The Criminal Law System*, 17 STAN. L. & POL'Y REV. 415, 420 (2006) (citing, *e.g.*, COMM'N ON INTELLIGENCE CAPABILITIES OF THE U.S. REGARDING WEAPONS OF MASS DESTRUCTION (THE WMD COMMISSION), REPORT TO THE PRESIDENT (2005); 9/11 COMMISSION REPORT, *supra* note 43; S. SELECT COMM. ON INTELLIGENCE & H. PERMANENT SELECT COMM. ON INTELLIGENCE, JOINT INQUIRY INTO INTELLIGENCE COMMUNITY ACTIVITIES BEFORE AND AFTER THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, S. REP. NO. 107-351, H. REP. NO. 107-792, 2d Sess. (2002); COMM'N ON ROLES AND

overstated[60] in the campaign for expanded surveillance powers immediately after 9/11, the confusion generated by the FISA wall hindered the sharing of intelligence necessary for the early detection of terrorist plots.[61]

The primary purpose test also failed to accomplish its driving goal of protecting First and Fourth Amendment rights. The lack of any probable cause requirement for a FISC order and the low standard of judicial review for assertions in FISA applications essentially gave law enforcement personnel carte blanche to obtain FISA warrants against anyone.[62] Indeed, FISC was called the "rubberstamp court" by many members of the intelligence community,[63] probably due to the fact that between 1979 and 2001 FISC approved all 14,036 applications submitted by the Executive branch.[64] The fact that FISC never turned down an application in the first twenty-three years of its existence[65] is especially troublesome given the revelation

---

CAPABILITIES OF THE U.S. INTELLIGENCE CMTY. (THE ASPIN-BROWN COMMISSION), PREPARING FOR THE 21ST CENTURY: AN APPRAISAL OF U.S. INTELLIGENCE (1996)).

60. *But see, e.g.*, SENATOR PATRICK LEAHY ET AL., INTERIM REPORT ON FBI OVERSIGHT IN THE 107TH CONGRESS BY THE SENATE JUDICIARY COMMITTEE: FISA IMPLEMENTATION FAILURES 15–21, 33, 35–36 (2003), *available at* http://grassley.senate.gov/releases/2003/p03r02-25c.pdf. This report identified "a failure to analyze and disseminate information within the FBI's possession" as well as a misunderstanding regarding the proper legal standard necessary for a FISA warrant as the true causes of the failure to detect Moussaoui's ultimate intentions. *Id.* at 6. Indeed, the report blamed a cumbersome FBI bureaucracy, an ineffective computer system which prevented agents from searching case files for key words, and a "deep rooted culture of ignoring problems" within the FBI as the primary barriers to cooperation and effective intelligence sharing. *Id.*; *see also* Banks, *Secret Surveillance*, *supra* note 9, at 1150 ("Largely lost in the rush to supply correctives to the failures in information-sharing and cooperation in the weeks and months after September 11 was the reality that laws were responsible only in a limited way for erecting a wall to effective inter-agency or law enforcement/intelligence community information-sharing. An institutional tradition hostile to coordination in large part created the wall." (citation omitted)); 9/11 COMMISSION REPORT, *supra* note 43, at 273–76 (identifying a failure to share information between the various intelligence agencies as one cause of 9/11 but refusing to blame any shortcomings in investigating Moussaoui on the FISA purpose requirement); Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. & POL'Y REV. 531, 535–36 (2006) (stating that "most of the bureaucratic obstacles had nothing to do with FISA, and some of the segmentation attributed to FISA was in fact the product of unrelated agency practices").

61. *See supra* notes 49–52.

62. *See supra* text accompanying notes 42–47 (outlining the requirements contained in Attorney General Janet Reno's 1995 memorandum which later became known as the FISA wall).

63. *See* Bungard, *supra* note 54, at 2.

64. *See* Michael P. O'Connor & Celia Rumann, *Going, Going, Gone: Sealing the Fate of the Fourth Amendment*, 26 FORDHAM INT'L L.J. 1234 (2003) (compiling the results from the annual reports of the Attorney General from 1979 to 2001, *available at* http://fas.org/irp/agency/doj/fisa).

65. FISC turned down no applications from 1979 to 2002 and has only turned down nine applications from 2003 to 2007. *See* Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Orders 1979–2002*, http://epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Nov. 7, 2008); *see also* Bungard, *supra* note 54, at 2; Nola K. Breglio,

in 2002 that the Justice Department admittedly knew of at least seventy-five instances where it provided false or misleading information in order to obtain approval for surveillance.[66] Significantly, one FBI agent was barred from appearing before the FISC due to repeated misstatements[67] and the person responsible for reviewing all FISA applications and summarizing this information for the benefit of the Attorney General was convicted of cocaine possession and making false statements.[68]

The primary purpose test also failed to confine the discretion of the executive to utilize FISA in criminal prosecutions unrelated to national security.[69] The concept underlying the test was that officers would be unable to utilize FISA surveillance in a criminal prosecution unless the discovery of the criminal evidence was

---

Note, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 YALE L.J. 179, 188 n.54 (2003); Federation of American Scientists, *Foreign Intelligence Surveillance Act, FISA Annual Reports to Congress*, http://fas.org/irp/agency/doj/fisa/#rept (last visited Nov. 8, 2008).

66. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620 (FISA Ct. 2002); *see also* Letter from William D. Delahunt, House Representative from Massachusetts, to Robert S. Mueller, Director of the FBI (June 14, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/del061402.pdf; Letter from M.E. Bowman, Deputy General Counsel for National Security Affairs, Office of the General Counsel, to Congressman William Delahunt (Aug. 7, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/ec.pdf.

67. *See In re All Matters Submitted*, 218 F. Supp. 2d at 621.

68. United States v. Barr, 963 F.2d 641, 644–46 (3rd Cir. 1992).

69. For over twenty-four years, from 1978 to 2001, the federal courts universally upheld FISA as an adequate substitute for a criminal warrant, satisfying the Fourth Amendment's reasonableness requirement, because of the government's "special needs" in national security investigations. *See In re* Sealed Case, 310 F.3d 717, 737 (FISA Ct. Rev. 2002) ("Senator Leahy believed that '[n]o matter what statutory change is made . . . the court may impose a constitutional requirement of "primary purpose" based on the appellate court decisions upholding FISA against constitutional challenges over the past 20 years.'" (quoting 147 Cong. Rec. S11003 (Oct. 25, 2001)); *see also* United States v. Duggan, 743 F.2d 59, 73 (2d Cir. 1984) ("procedures established in [FISA] are reasonable in relation to legitimate foreign counterintelligence requirements and the protected rights of individuals" and therefore are constitutional); United States v. Cavanagh, 807 F.2d 787, 789–90 (9th Cir. 1987); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987). However, these courts viewed this exception to the Fourth Amendment as applicable only if the government's primary purpose was national security collection. *See, e.g.*, United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Pelton, 835 F.2d 1067, 1075–76 (4th Cir. 1987); United States v. United States District Court (Keith), 407 U.S. 297, 322–23 (1972); *see also* THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978: THE FIRST FIVE YEARS, S. REP. NO. 98-660, at 15 (1984) ("[T]he Justice Department should use Title III when it is clear that the main concern with respect to a terrorist group is domestic law enforcement and criminal prosecution, even if the surveillance will also produce some foreign intelligence information."); Banks, *Secret Surveillance*, *supra* note 9, at 1160 (discussing the placement of FISA in Title 50, War and National Defense, as demonstrating congressional intent and noting that "Congress did not intend for FISA to in any way authorize surveillance for law enforcement purposes").

inadvertent.[70] In practice, however, the primary purpose test did not result in a searching judicial inquiry into the subjective motivations of the law enforcement personnel conducting the search and no court suppressed evidence generated from FISA surveillance.[71]

The primary purpose test lacked teeth for two fundamental reasons. First, courts were ill-equipped to evaluate the subjective motivations of officers conducting surveillance[72] and preferred to draw bright line rules. In this case, the bright line "wall" established by Janet Reno's 1995 procedures satisfied most courts. Second, the primary purpose test rested "on a false premise" that foreign intelligence gathering is entirely distinct from criminal investigation.[73] The line developed in the *Truong* case was "inherently

70. *See* Gregory E. Birkenstock, *The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis*, 80 GEO. L.J. 843, 861 (1992) ("When FISA was being drafted, the Judiciary Committee expected 'relatively few' cases in which materials unearthed under FISA would be used as evidence in criminal prosecutions."); S. REP. No. 95-604, pt. 1, at 52–53 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3954 ("[U]ses to be made of the [FISA] information acquired by means of this chapter [must] be carefully restricted.").

71. *See supra* notes 64–65. None of the cases interpreting FISA from 1978 to 2001 found the primary purpose of the surveillance to be criminal prosecution and excluded evidence on this basis; *see, e.g.*, United States v. Sarkissian, 841 F.2d 959, 965 (9th Cir. 1988) (declining to decide whether the test is one of purpose or primary purpose and refusing "to draw too fine a distinction between criminal and intelligence investigations. 'International terrorism,' by definition, requires the investigation of activities that constitute crimes."); United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987); *Badia*, 827 F.2d at 1464 (holding that "the telephone surveillance of Arocena did not have as its purpose the primary objective of investigating a criminal act. Rather, surveillance was sought for the valid purpose of acquiring foreign intelligence information."); United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984) (stating that "the requirement that foreign intelligence information be the primary objective of the surveillance is plain not only from the language of § 1802(b) but also from the requirement in § 1804 as to what the application must contain." In this case, however, the primary purpose test was satisfied because "otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of such surveillance may later be used, as allowed by § 1806(b), as evidence in a criminal trial."); United States v. Rahman, 861 F. Supp. 247, 252 (S.D.N.Y. 1994) ("There is no contradiction, indeed there probably is often a congruence, between foreign intelligence information and evidence of criminal wrongdoing. That does not mean the government may not avail itself of FISA in order to protect national security when to do so will also generate evidence that may be used in a criminal case."); United States v. Johnson, CRIM. A. No. 89-221-MA, 1990 WL 78522 (D. Mass. Apr. 13, 1990); *In re* Matter of Kevork, 634 F. Supp. 1002 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986) (holding that the primary purpose test was satisfied by the evidence in this case); United States v. Falvey, 540 F. Supp. 1306, 1311 (E.D.N.Y. 1982) (upholding the use of electronic surveillance evidence "[w]hen, therefore, the President has, as his *primary purpose*, the accumulation of foreign intelligence information") (emphasis added).

72. Fourth Amendment inquiries typically ignore the subjective motivation of the officer involved in the search. *See* Whren v. United States, 517 U.S. 806, 813 (1996) (holding that the constitutionality of a traffic stop does not depend upon the subjective intent of the officer). As discussed below, the requirement that the officer "inadvertently" discover evidence in the context of "plain view" searches, was vitiated by Horton v. California, 496 U.S. 128, 138–42 (1990).

73. *In re* Sealed Case, 310 F.3d 717, 743 (FISA Ct. Rev. 2002).

unstable, unrealistic, and confusing"[74] because it was impossible to separate gathering intelligence and fighting national security crimes.[75] A typical foreign intelligence investigation begins with the FBI keeping tabs on foreign groups even though the FBI may lack probable cause of any anticipated criminal activity. At some point, the surveillance may generate evidence of a foreign intelligence crime such as espionage or terrorism but this does not transform the purpose of the surveillance. Indeed, protecting national security and detecting crimes often go hand-in-hand; terrorism is defined by FISA as violent activity which "would be a criminal violation if committed within . . . the United States or any State."[76] In most cases, it will be impossible to determine the point at which the government decides that criminal prosecution is the appropriate means of proceeding. Finally, the increased criminalization of terrorism-related crimes[77] in recent years makes it more difficult to parse the government's objectives in any particular case.[78]

III. THE PATRIOT ACT AND THE SHIFT TO A "SIGNIFICANT PURPOSE" TEST

Only six weeks after the September 11th attacks, President George W. Bush signed the Patriot Act[79] and authorized a series of

74. *Id.*

75. *Id.* (Those cases implementing the "primary purpose" test relied on "the false premise . . . that once the government moves to criminal prosecution, its 'foreign policy concerns' recede . . . . [C]riminal prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts. Indeed, . . . 'almost all foreign intelligence investigations are in part criminal investigations.'" (quoting United States v. Truong, 629 F.2d 908, 915 (4th Cir. 1980))).

76. 50 U.S.C. § 1801(c) (2000).

77. NORMAN ABRAMS, ANTI-TERRORISM AND CRIMINAL ENFORCEMENT 5–7 (1st ed. 2005) (arguing that in the years since FISA was implemented, Congress has criminalized more and more national security and terrorism-related conduct, adding hundreds of new offenses to the federal criminal code).

78. *See, e.g.*, United States v. Sarkissian, 841 F.2d 959, 965 (9th Cir. 1988) (refusing to affirm the primary purpose test because the distinction between foreign intelligence surveillance and criminal investigations is almost immaterial and acts of international terrorism ultimately entail criminal investigations because terrorism is also a criminal offense).

79. Critics of the Patriot Act have argued that the rush to "do something" led to a lack of thoughtful debate and adequate consideration of the monumental changes being enacted. *See* David Hardin, *The Fuss Over Two Small Words: The Unconstitutionality of the USA Patriot Act Amendments to FISA Under the Fourth Amendment*, 71 GEO. WASH. L. REV. 291, 319 (2003) ("Given the magnitude of the USA PATRIOT Act in affecting our civil liberties, however, the time and scrutiny afforded this historical legislation raises concerns of its legitimacy and constitutionality . . . . Just 36 days after the legislation's introduction, Congress 'rubber-stamped' it after making only minor alterations. The rush to pass the bill was so swift that on the day the House had its final debate, members complained that they did not have a chance to read the final version." (internal citations omitted)).

sweeping changes undermining the balance between individual rights and government power embodied in the original 1978 FISA statute.[80] Not only did the Patriot Act authorize roving wiretaps, internet tracking, and "sneak-and-peek"[81] searches, but it also removed any teeth from the *Truong* primary purpose test.[82] Prior to the Patriot Act, the applicant had to certify that the "the purpose of the surveillance [was] the collection of foreign intelligence," but after the Patriot Act's amendments to FISA, the applicant only had to certify that "a significant purpose of the surveillance is the collection of foreign intelligence."[83] Congress made clear its intention to break down the "primary purpose" wall by specifically authorizing the sharing of information between intelligence and law enforcement officials without OIPR supervision.[84]

Shortly after the passage of the Patriot Act, Attorney General John Ashcroft issued a memorandum in March 2002 explicitly repudiating the 1995 guidelines and allowing prosecutors to "direct and control" FISA surveillance.[85] In a subsequent appeal to the Foreign Intelligence Surveillance Court of Review ("FISCR"), the secret FISA review court approved the Attorney General's proce-

80. Stephanie Kornblum, Note, *Winning the Battle While Losing the War: Ramifications of the Foreign Intelligence Surveillance Court of Review's First Decision*, 27 SEATTLE U. L. REV. 623, 624 (2003) ("Prohibiting that interaction [between law enforcement and foreign intelligence officials] is one way in which the statute seeks to balance individual liberties while providing the government the ability to conduct surreptitious surveillances, an invaluable tool in terrorism and espionage investigations."); *see also* Banks, *Death of FISA*, *supra* note 40, at 1215 ("[T]he central premise of the FISA compromise—authorizing secret electronic surveillance for the purpose of collecting foreign intelligence, but subjecting applications to judicial scrutiny and the entire process to congressional oversight has been lost." (citing 18 U.S.C. § 2511(2)(f) (2006))); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1325 (2004) (stating that the 1978 FISA "revealed a grand compromise between advocates for civil liberties and the intelligence community").

81. A "sneak-and-peak" search warrant authorizes law enforcement officers to enter a private premises, without the owner or occupant's permission or knowledge and clandestinely search the premises and seize any materials found within the premises. *See* USA PATRIOT ACT, Pub. L. No. 107-56, § 213, 115 Stat. 272, 285–86 (2001) (amending 18 U.S.C. § 3103(a) (2006)).

82. *See* Kornblum, *supra* note 80, at 627 ("This seemingly small change in wording has potentially great impact. FISA's relaxed probable cause requirement was previously reserved for situations where the only purpose was foreign intelligence gathering. The new wording allows the government to avoid the normal probable cause required to obtain a warrant in a criminal investigation.").

83. USA PATRIOT ACT, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (2001) (amending 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2000)).

84. *Id.* § 504 (codified as amended at 50 U.S.C. § 1806(k) (West Supp. 2002)).

85. Memorandum from John Ashcroft, U.S. Attorney General, to Director of the FBI, Assistant Attorney General for the Criminal Division, Counsel for Intelligence Policy, and United States Attorneys, (Mar. 6, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/ag030602.html.

dures.[86] The court concluded: "[t]he addition of the word 'significant' to section 1804(a)(7)(B) imposed a requirement that the government have a *measurable* foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes."[87]

The FISCR court's reading of the significant purpose test only requires the government to retain "a realistic option of dealing with the agent other than through criminal prosecution"[88] and, as a result, the government will likely satisfy this test in every case.[89] It is extremely difficult to conceive of a case in which the government is monitoring a person and yet would not have a measurable foreign intelligence purpose even if criminal prosecution is inevitable.[90] For example, the government would have a "measurable foreign intelligence purpose" if prosecutors indict the target with the hope they can turn the target into a valuable informant. Alternatively, the government may be ready to proceed with prosecution but wait to see if the target accidentally reveals other sources or contacts. The inadequacy of the "significant purpose" standard is further compounded by the fact that a court deciding whether to admit evidence gathered pursuant to a FISA warrant in a criminal proceeding can only review the FISC determination of the purpose of the surveillance for "clear error."[91]

Critics of the shift to the "significant purpose" test deride it as creating an "end run" around the Fourth Amendment, allowing prosecutors to avoid the constitutionally mandated protections of Title III simply by certifying that the target of the surveillance is an

86. *In re* Sealed Case, 310 F.3d. 717, 730 (FISA Ct. Rev. 2002).

87. *Id.* at 734 (emphasis added).

88. *Id.*

89. *See* O'Connor & Rumann, *supra* note 64, at 1262–63 ("The FISCR has effectively told us that the Constitution need not control the conduct of criminal surveillance in the United States."); George P. Varghese, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385, 429 (2003) ("On November 18, 2002, the FISCR granted the government a new and incredibly powerful tool in the war on terror at the expense of the Fourth Amendment. By upholding the Patriot Act and the 2002 Procedures, the FISCR permitted, for the first time, the use of the foreign intelligence exception to bypass the constitutional rights of U.S. citizens targeted in law enforcement investigations.").

90. *See* Hardin, *supra* note 79, at 343 ("[T]he new foreign intelligence purpose standard disables the FISC or any other court from ascertaining the existence of a foreign intelligence purpose in light of the ambiguity inherent in the term 'significant' and the broad nature of acts that may lead to probable cause under FISA.").

91. 50 U.S.C. § 1805(a)(5) (2000); *see, e.g.*, United States v. Rahman, 861 F. Supp. 247, 251 (S.D.N.Y. 1994) (stating that "a reviewing court is not to 'second-guess' the [government's] certification" that the primary purpose of the surveillance is the collection of foreign intelligence information).

agent of a foreign power.[92] For the first time, during the 2003 and 2004 calendar year, the number of surveillance orders granted under FISA exceeded the number granted under Title III, providing some factual support for the claim that FISA will gradually replace Title III as the primary vehicle for authorizing surveillance.[93] Even the FISC court has noted: "[t]he 2002 procedures appear to be designed to amend the law and substitute FISA for Title III electronic surveillances and Rule 41 searches. This may be because the government is unable to meet the substantive requirements of these law enforcement tools."[94]

In the context of certain crimes, such as espionage, sabotage and terrorism, the pretextual use of FISA to gather evidence primarily intended for use in a criminal trial may seem like a minor concern. After all, pretextual surveillance will only detect evidence of crimes that are being committed, and the government's interest in preventing terrorism, sabotage, and espionage is clearly paramount. A major concern, however, should be FISA's specific

92. *See, e.g.*, Petition for Leave to Intervene and Petition for a Writ of Certiorari of American Civil Liberties Union et al., *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (No. 02-001) [hereinafter ACLU Petition]; O'Connor & Rumann, *supra* note 64; Risa Berkower, Note, *Sliding Down a Slippery Slope? The Future Use of Administrative Subpoenas in Criminal Investigations*, 73 FORDHAM L. REV. 2251, 2280–87 (2005); James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1492 (2004) ("The fear is that having developed an effective and justified analytic tool and gained access to commercial sources of information for counterterrorism purposes, an agency or other agencies will then seek to use the information for purposes extending beyond counterterrorism, purposes that on their own would not have supported access to the information, but that seem to offer benefits at a marginal cost once the information is available.").

93. While it is certainly true that this increase may be a result of an increased number of terrorism investigations, it also supports the argument that FISA is being used in some borderline cases. *See* Nicholas Whilt, *The Foreign Intelligence Surveillance Act: Protecting the Civil Liberties that Make Defense of our Nation Worthwhile*, 35 SW. U. L. REV. 361, 394 (2006) [hereinafter Whilt] (compiling the results of Administration Office of the U.S. Cts); *see also* Letter from William E. Moschella, Assistant Attorney General, to L. Ralph Mecham, Director, Administrative Office of the United States Courts, (Apr. 30, 2004), *available at* http://www.fas.org/irp/agency/doj/fisa/2003rept.pdf (reporting that during the 2003 calendar year, the FISC approved 1,724 FISA applications); Letter from William E. Moschella, Assistant Attorney General, to Hon. J. Dennis Hastert, Speaker, United States House of Representatives, (Apr. 1, 2005), *available at* http://www.fas.org/irp/agency/doj/fisa/2004rept.pdf (reporting that during the 2004 calendar year, the FISC approved 1,754 applications to conduct FISA surveillance); Administrative Office of the United States Courts, 2004 Wiretap Report, *available at* http://www.uscourts.gov/wiretap04/contents.html (reporting that during the 2004 calendar year, the federal courts approved 1,710 applications to conduct surveillance under Title III).

94. *In re* All Matters Submitted, 218 F. Supp. 2d 611, 623 (FISA Ct. 2002). The court further hypothesized that prosecutors, who can now direct and control a FISA investigation, may seek a FISA warrant in ordinary criminal cases when they lack probable cause; "criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence." *Id.* at 624.

authorization of the use of FISA surveillance evidence in criminal prosecutions of non-foreign intelligence crimes.[95] As a result, a law enforcement person could circumvent the constitutional protections of Title III by obtaining a FISA warrant, without probable cause, to prosecute a person suspected only of "ordinary" criminal activity.[96]

One fear is that FISA will be used pretextually to target innocent Arab-Americans and Muslims and that the evidence obtained from FISA surveillance will be used disproportionately to prosecute these minority groups for drug crimes, gun possession, immigration violations, and minor crimes. Another worry is that FISA could be used to target political opponents, thereby chilling political speech.

Even if the "significant purpose" test is satisfied in every case, the government must still certify that the FISA target is the "agent of a foreign power."[97] This requirement, however, is also easily satisfied. Under 50 U.S.C. § 1801(b),[98] a person can qualify as an agent of a foreign power if he (1) acts as a member of a foreign power; (2) knowingly engages in clandestine intelligence gathering which *may* involve a violation of the criminal laws of the U.S. or in the case of

95. FISA specifically authorizes the retention of information that is "evidence of a crime," 50 U.S.C. § 1801(h)(3) (2000), and provides procedures for the retention and dissemination of such information. 50 U.S.C. § 1806(b)-(f) (2000). There is no requirement that the "crime" be related to foreign intelligence and courts have allowed the use of FISA materials in prosecutions of non-foreign intelligence crimes. *See* United States v. Wen, 477 F.3d 896, 898 (7th Cir. 2007) ("If, while conducting this surveillance, agents discover evidence of a domestic crime, they may use it to prosecute for that offense. That the agents may have known that they were likely to hear evidence of domestic crime does not make the interception less reasonable than if they were ignorant of this possibility. Justice Stewart's position that the plain-view doctrine is limited to 'inadvertent' discoveries, has not carried the day."); United States v. Isa, 923 F.2d 1300, 1302, 1304–06 (8th Cir. 1991) (admitting evidence obtained during FISA surveillance in an unrelated murder prosecution); United States v. Hawamda, No. 89-56-A, 1989 WL 235836, at *2 (E.D. Va. Apr. 17, 1989) ("[W]hen a monitoring agent overhears evidence of domestic criminal activity, it would be a subversion of his oath of office if he did not forward that information to the proper prosecuting authorities.").

96. *Cf.* Coolidge v. New Hampshire, 403 U.S. 443, 466–68 (1971) (plurality opinion) (arguing that if the police know that they can use legal authority to search for one thing as a way of looking for another thing, they may embark on pretextual searches and fishing expeditions); Horton v. California, 496 U.S. 128, 138–40 (1990) (rejecting a subjective intent test for the plain view exception but recognizing that the possibility of officers using plain view to execute pretextual searches is a legitimate Fourth Amendment concern).

97. Although, as a result of the FISA Amendment of 2008, even this requirement is inapplicable in the context of surveillance of persons reasonably believed to be located outside of the United States. *See* H.R. 6304, 110th Cong. § 702(b) (2008), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h6304enr.txt.pdf.

98. *See supra* note 15.

non-U.S. persons[99] circumstances indicate that he *may* engage in clandestine intelligence gathering; or (3) knowingly engages in international terrorism or sabotage.[100] While this definition appears to limit FISA surveillance to a narrow range of people, in reality its broad terms capture quite a large group of people.[101] A "foreign power," for example, includes a component of a foreign government, a foreign political organization, or an entity that is directed or controlled by a foreign government.[102] "International terrorism" is defined as "violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State."[103] In addition, the Patriot Act's "lone wolf" provision essentially qualifies any non-citizen, acting alone, as an "agent of a foreign power."[104] Based on this provision, "suspected terrorists may be targeted under FISA even if there is no proof of a connection to any terrorist group or a foreign power."[105]

These amorphous definitions cover such a broad range of activity that overzealous law enforcement personnel will have little trouble fitting U.S. citizens into one of the aforementioned categories.[106] Finally, non-U.S. citizens are afforded no protection under FISA because the FISC judges cannot question or scrutinize the

---

99. The term "U.S. persons" includes both U.S. citizens and legal permanent residents of the United States. *See* 50 U.S.C. § 1801(i) (2000).

100. *See supra* note 15.

101. *See, e.g.*, O'Connor & Rumann, *supra* note 64, at 1258 ("The first thing that should be apparent is the incredible breadth of these definitions. . . . The terms used above include definitions of criminal behavior so broad, as to encompass any violation of the criminal statutes of the United States, and any violent act which would violate the criminal law of the United States or any State.").

102. 50 U.S.C. § 1801(a) (2000).

103. *Id.* § 1801(c).

104. As amended, the "[a]gent of a foreign power" may include any person, other than a United States person, who "engages in international terrorism or activities in preparation therefore." 50 U.S.C. § 1801(b)(1)(C) (2000); *see* ELIZABETH B. BAZAN, CONGRESSIONAL RESEARCH SERVICE, CRS INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004: "LONE WOLF" AMENDMENT TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT REPORT TO CONGRESS (2004), *available at* http://www.fas.org/irp/crs/RS22011.pdf.

105. Banks, *Death of FISA*, *supra* note 40, at 1274 ("[I]n the post-September 11 era, where supposed links to al Qaeda are legion, the tendency to rely on FISA to investigate even the most speculative suspicions of a connection to international terrorism by lone wolves could turn FISA surveillance into a quotidian occurrence.").

106. *See* O'Connor & Rumann, *supra* note 64, at 1258 (arguing that the definition of international terrorism is broad enough to capture any criminal violation and therefore provides no safeguard against the pretextual use of FISA); Varghese, *supra* note 89, at 427 (arguing that "[t]he statutory definition leaves open the possibility that a U.S. citizen may be involved in clandestine intelligence activities that do not involve criminal conduct at all" and that "while the statute clearly contemplates crimes like espionage, any violation of the criminal statutes, no matter how minor, would fall within its definition"); *see also* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984) (defendants argued that FISA allowed surveillance of persons "who may be engaging in activities that 'may' violate United States law").

assertions of the executive branch and therefore, they simply review the application for procedural regularity.[107] It is almost impossible to conceptualize a situation in which a FISC judge will find an application to be "clearly erroneous" during an *ex parte* proceeding; to date, no applicant has been successful in challenging a FISA application in the subsequent criminal proceeding.[108] These expansive definitions, coupled with the history of false statements, omissions, and mischaracterizations of evidence by FISA applicants, certainly lend credibility to the claim that, without the safeguards provided by the primary purpose test, FISA will increasingly be used as a way to circumvent the strict requirements of Title III.

Non-U.S. citizens and American citizens of foreign descent will likely be the people most frequently ensnared by the over-breadth of these definitions.[109] The definition of a foreign agent is designed to be easier to satisfy in the case of aliens and there is no judicial review of the executive's certifications provided for non-U.S. citizens.[110] In addition, the FISA Amendment of 2008 enables the government to monitor the communications of any person "reasonably believed to be located outside of the United States" without presenting any evidence that this person is "an agent of a foreign power."[111] The amorphous restrictions on this loophole make it likely that anytime a U.S. citizen places an international call or sends an international email, they are forfeiting some

107. *See supra* text accompanying notes 20–24.

108. *See, e.g.*, United States v. Isa, 923 F.2d 1300 (8th Cir. 1991); United States v. Badia, 827 F.2d 1458 (11th Cir. 1987); Duggan, 743 F.2d 59; United States v. Holy Land Found. for Relief and Dev., No. 3:04-CR-240-G, 2007 WL 2011319 (N.D. Tex. July 11, 2007); United States v. Rosen, 447 F. Supp. 2d 538 (E.D. Va. 2006); United States v. Jamal, 285 F. Supp. 2d 1221 (D. Ariz. 2003); United States v. Rahman, 861 F. Supp. 247 (S.D.N.Y. 1994).

109. For example, Senator Russ Feingold, (D-Wisconsin), the only Senator to vote against the Patriot Act, said: "[W]ho do we think is most likely to bear the brunt of the abuse? It won't be immigrants from Ireland, it won't be immigrants from El Salvador or Nicaragua, it won't even be immigrants from Haiti or Africa. It will be immigrants from Arab, Muslim and South Asian countries. In the wake of these terrible events our government has been given vast new powers and they may fall most heavily on a minority of our population who already feel particularly acutely the pain of this disaster." Robert N. Davis, *Striking the Balance: National Security vs. Civil Liberties*, 29 BROOK. J. INT'L L. 175, 217 (2003) (citing Sen. Russell Feingold, *Statement on the Anti-Terrorism Bill*, (Oct. 25, 2002), Electronic Privacy Information Center, *available at* http://www.epic.org/privacy/terrorism/usapatriot/feingold.html).

110. 50 U.S.C. § 1805(a)(5) (2000); *see also* United States v. Megahey, 553 F. Supp. 1180, 1198–1200 (E.D.N.Y. 1982), *aff'd*, Duggan, 743 F.2d at 75–77 (rejecting the defendant's argument that the different treatment of aliens and non-aliens is a violation of equal protection).

111. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 701(g)(1)(B), 122 Stat. 2436, 2440 (2008).

Fourth Amendment protection.[112] This new amendment seems most likely to result in increased surveillance of recent immigrants and other residents with ties to foreigners. It also seems logical to assume that the government is more likely to seek FISA warrants for the surveillance of Muslim and Arab citizens. A Muslim citizen who belongs to a religious organization or a semi-political group could be classified as being a "member" of a "foreign political organization."[113] In *Zweibon v. Mitchell*, the court noted that even limiting warrantless surveillance to cases involving agents of foreign powers would fail to protect First Amendment rights because "under such a test, a few alien members in a political organization would justify surveillance of the conversations of all members."[114] The court offered as an example its view that, under such a test, antiwar organizations sponsoring speeches by South Vietnamese political dissenters during the 1960's could have been wiretapped without a warrant.[115] This discriminatory abuse of the government's power to search and surveil its citizens was exactly the type of practice the Fourth Amendment was designed to prohibit.[116]

The potential for abuse of this broad discretion becomes especially worrisome in cases involving the intersection of political speech, religion, and race. The targeting of members of pro-Palestinian political groups is one example.[117] As discussed above, FISA does not define the term "clandestine intelligence gathering"

---

112. The government is required to *certify* that they are not intentionally targeting a person located within the United States and adopt targeting procedures to ensure that they are "targeting" persons located outside the United States and to prevent the intentional acquisition of calls between two persons in the United States. § 702(d)-(e). The FISC court also reviews these procedures to ensure that they contain all the requisite elements and that the targeting procedures are reasonable. § 702(i). These requirements do not, however, prevent the government from monitoring calls made by U.S. citizens located in the United States to persons reasonably located outside of the United States, so long as the government is targeting the non-U.S. citizen.

113. *See* Grayson A. Hoffman, Note, *The New FISA Regime, The Wall, and the Fourth Amendment*, 40 AM. CRIM. L. REV. 1655, 1674 (2003) (demonstrating that "a federal prosecutor theoretically could secure a FISA surveillance order to monitor an American citizen residing in the United States who joined a pro-Palestinian movement with a history of staging violent protests. The prosecutor could seek FISA surveillance on the basis that, inter alia, the target's behavior 'may involve' criminal activity.").

114. 516 F.2d 594, 635 (D.C. Cir. 1975).

115. *Id.*

116. *See generally* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 94–95 (Johns Hopkins Press ed., 1937).

117. *See* Whilt, *supra* note 93, at 393 ("This is problematic because a United States citizen could be a member of the Palestine Liberation Organization, or a foreign website where members discuss political views, and such an organization would qualify as 'a foreign based political organization, not substantially composed of United States persons.' As such, the members could be considered engaged in 'clandestine intelligence gathering activities' for conducting legitimate research . . . to learn about U.S. policy toward their political views.").

and its definition of international terrorism includes legal activity that "may" constitute a crime.[118] Therefore, the opportunity exists for law enforcement personnel to target political opponents for activity the government considers to be the "gathering of intelligence" or for advocating a change in existing foreign policy.[119] Even without imputing evil motives to the government, it is easy to imagine a reporter communicating with sources in Afghanistan or Iraq being identified by the TSA data-mining program as a potential threat and this alone warranting a FISA wiretap.[120] Equally distressing is the chilling effect these vague definitions may have on constitutionally protected political speech. The ACLU, in its brief to the FISCR, argued: "[e]xpanding the circumstances in which the government may invade the individual's protected sphere without probable cause also presents the danger that the government's surveillance power will chill dissent, and indeed that the government may wield its power with the specific intent of chilling dissent."[121] The Supreme Court has recognized that: (1) the executive will be inclined to target political opponents; and (2) if people know that their government can spy on them without probable cause they will almost certainly chill their dissenting political speech.[122] Indeed, the executive abuses in targeting political

118. Varghese, *supra* note 89, at 420 ("The statutory definition leaves open the possibility that a U.S. citizen may be involved in clandestine intelligence activities that do not involve criminal conduct at all.").

119. *Zweibon*, 516 F.2d at 635 n.107 (arguing that under the permissive definition of an "agent of a foreign power," "even a domestic political leader could be wiretapped without a warrant if the Government believed he had wittingly or unwittingly become the 'agent' of a foreign power").

120. For example, Lawrence Wright, author of *The Looming Tower*, a Pulitzer Prize-winning book on al-Qaeda, reported that two members of an FBI terrorism task force showed up at his house in 2002 while he was researching the book and interrogated him regarding his daughter's alleged communications with al-Qaeda operatives. It later became clear to Mr. Wright that they had been "monitoring" his phones and storing portions of his conversations. *See* Lawrence Wright, *The Spymaster: Can Mike McConnell Fix America's Intelligence Community?*, THE NEW YORKER, Jan. 21, 2008, *available at* http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright?currentPage=all.

121. ACLU Petition, *supra* note 92, at 44. FISA does contain a provision which prohibits the probable cause finding that a United States person is an agent of a foreign power from resting "solely upon the basis of activities protected by the [F]irst [A]mendment to the Constitution of the United States" but it is unclear how much work this provision does towards preventing the pretextual use of FISA given the minimal judicial scrutiny afforded defendants under 50 U.S.C. § 1805(a)(5) (2000). *See infra* text accompanying notes 20–26.

122. United States v. United States District Court (Keith), 407 U.S. 297, 314 (1972) ("History abundantly documents the tendency of Government-however benevolent and benign its motives-to view with suspicion those who most fervently dispute its policies."); *see also* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 491–99 (2006) (discussing negative effects of surveillance); *Zweibon*, 516 F.2d at 635–36 (warning that allowing the executive branch to make its own determinations regarding warrantless surveillance "invites

opponents documented in the Church Committee reports, which inspired FISA's enactment, provide historical support for this argument.[123]

After 9/11, the need to preemptively detect terrorist plots and coordinate all of the resources of the federal government may have warranted the shift to the significant purpose test and, indeed, according to the government this shift has already paid dividends in preventing several terrorist attacks.[124] At the same time, electronic surveillance technology has advanced at an astounding rate and is now more intrusive then ever before. For example, the government can store and search massive amounts of emails, follow a suspect's web-browsing history,[125] and track a suspect's movement via his cell phone.[126] In addition, the resources directed at counter-

abuse, and public knowledge that such abuse is possible can exert a deathly pall over vigorous First Amendment debate on issues of foreign policy").

123. *See, e.g.*, the concerns regarding the enactment of the Patriot Act expressed by the former Clinton White House Chief of Staff, John Podesta, *USA PATRIOT Act: The Good, the Bad, and the Sunset*, 29 HUM. RTS. MAG. 3, 7 (2002) ("We should not forget what gave rise to the original opposition—many aspects of the [Patriot Act] increase the opportunity for law enforcement and the intelligence community to return to an era where they monitored and sometimes harassed individuals who were merely exercising their First Amendment rights. Nothing that occurred on September 11 mandates that we return to such an era.").

124. *See* Banks, *The Death of FISA*, *supra* note 40, at 1299–1300 (according to Banks, "[t]he Justice Department has proudly showcased what it views as the tremendous benefits from the Patriot Act's information sharing provisions and the lowering of the wall. One example involved the Department's investigations of suspected al Qaeda cell members in Lackawanna, New York, the 'Lackawanna Six.' The investigation began in the summer of 2001 based on an anonymous tip delivered to the FBI that local Yemeni-Americans might be involved in drug crime and terrorist activities. Initially, the FBI 'concluded that existing law required the creation of two separate investigations in order to retain the option of using FISA.' According to the Department, the Patriot Act made clear that information sharing between the two teams was allowed, which in turn let the criminal side know that an al Qaeda agent was involved, leading to early criminal charges against the six.") (citing U.S. DEP'T OF JUSTICE, REPORT FROM THE FIELD: THE USA PATRIOT ACT AT WORK 3 (2004), *available at* http://www.fas.org/irp/agency/doj/patriot0704.pdf)). *But see* Banks, *Secret Surveillance*, *supra* note 9, at 1188 (questioning the government's assertions that the federal prosecution of a Florida professor and seven others for financing suicide bombings in Israel was only made possible by the expanded powers given to the Department of Justice after 9/11).

125. For example, Carnivore (later incarnations of which have been known as DCS-1000) is a "packet sniffer," an Internet wiretap that reads traffic while it is in transit in packet form. *See, e.g.*, Christian D. H. Schultz, Note, *Unrestricted Federal Agent: "Carnivore" and the Need to Revise the Pen Register Statute*, 76 NOTRE DAME L. REV. 1215, 1223–30 (2001) (providing an overview of the Carnivore system and its capabilities); John Schwartz, *Privacy Debate Focuses on F.B.I. Use of an Internet Wiretap*, N.Y. TIMES, Oct. 13, 2001, at A14 ("When Carnivore sits down to eat, it tastes everything . . . . Once installed at the offices of an Internet service provider, it works by monitoring all of the data that flows by it.").

126. The government is able to triangulate a suspect's location on the basis of "cell site" information (signals sent from a person's cell phone, even when not in use, to nearby cell towers). *See* Stephanie Lockwood, Recent Development, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308–16 (2004) (discussing the use of GPS positioning and signal triangulation to track a

ing terrorism have increased massively since September 11th and their focus has shifted toward intervening before an attack is committed.[127] The Patriot Act now authorizes "sneak-and-peak searches,"[128] roving wiretaps which follow a suspect as he changes phones, and access to "any tangible record" related to the target.[129] This expansion of executive power must be restrained by some method which protects individual rights while allowing the various branches of the government to share information and coordinate their efforts to prevent terrorist attacks.

IV. THE INEXTRICABLY INTERTWINED TEST

This Note proposes that information gathered pursuant to a FISA warrant be admitted only in those criminal cases involving terrorism, espionage, or sabotage; or, in those cases where the charges are "inextricably intertwined" with a foreign intelligence crime.[130] Evidence gathered pursuant to a FISA warrant would be

---

suspect's movements); Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L. J. 381, 384–94 (2003) (discussing recent advancements in cellular telephone location tracking technology and analyzing proposed legal restrictions on the technology). *Compare In re* Application of the United States For An Order For Disclosure of Telecommunication Records And Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435, 439–40, 449–50 (S.D.N.Y. 2005) (allowing the government to obtain cell-site information on a certification of less than probable cause), *with In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F. Supp. 2d 294, 305–10, 321–24 (E.D.N.Y. 2005) (refusing to authorize the acquisition of cell-site information on a showing of less than probable cause).

127. The Attorney General has described the Department of Justice as adding a new "paradigm of prevention" to that of prosecution. Banks, *Secret Surveillance*, *supra* note 9, at 1153 (citing Adam Liptak, *Under Ashcroft, Judicial Power Flows Back to Washington*, N.Y. TIMES, Feb. 16, 2003, at wk5).

128. "Sneak-and-peek" searches were authorized in the Second Circuit prior to the Patriot Act. *See* United States v. Pangburn, 983 F.2d 449, 455 (2d Cir. 1993) (declining to suppress evidence obtained pursuant to a "covert entry" warrant and stating that "[t]he Fourth Amendment does not deal with notice of any kind"); United States v. Villegas, 899 F.2d 1324, 1337–38 (2d Cir. 1990), *cert. denied*, 498 U.S. 991 (1990) (authorizing a covert entry search and requiring that notice of the search be given to the defendant "within a reasonable time after the covert entry" but accepting a delay of two months); United States v. Freitas, 800 F.2d 1451 (9th Cir. 1986), *modified*, 856 F.2d 1425 (9th Cir. 1988); *see also* Kevin Corr, *Sneaky but Lawful: The Use of Sneak and Peek Search Warrants*, 43 U. KAN. L. REV. 1103, 1105 (1995); Paul V. Konovalov, Note, *On a Quest for Reason: A New Look at Surreptitious Search Warrants*, 48 HASTINGS L.J. 435, 443 (1997).

129. Smith, *supra* note 16, at 416–23.

130. This Note argues that Congress should statutorily create a means of enforcing the FISCR's reasoning that FISA can only be used to investigate those crimes "inextricably intertwined" with a national security interest. *In re* Sealed Case, 310 F.3d 717, 736 (FISA Ct. Rev. 2002); *see also* Matthew R. Hall, *Constitutional Regulation of National Security Investigation:*

inadmissible in a prosecution for an "ordinary crime" with an insufficient nexus to national security. This proposed restriction on the use of evidence of unrelated crimes is not entirely without precedent. Several states restrict the use of plain view evidence inadvertently discovered pursuant to a Title III warrant[131] and language in the FISCR's most recent decision indicates that the court would support such a restriction. The court stated that FISA "cannot be used as a device to investigate wholly unrelated ordinary crimes" and dismissed the government's assertion that prosecution of non-terrorist related crimes would be consistent with the government's national security interest because it would incapacitate the agent of a foreign power.[132] The FISCR also would allow the admission of FISA evidence in a prosecution for a crime with a link to a foreign intelligence crime:

> That is not to deny that ordinary crimes might be inextricably intertwined with foreign intelligence crimes. For example, if a group of international terrorists were to engage in bank robberies in order to finance the manufacture of a bomb, evidence of the bank robbery should be treated just as evidence of the terrorist act itself.[133]

The FISCR, however, fails to further define which crimes would be "inextricably intertwined" with foreign intelligence crimes and it provides no mechanism for limiting the use of FISA material in non-foreign intelligence prosecutions. Indeed, no court before or after this decision has found FISA material to be inadmissible in the prosecution of an unrelated ordinary crime.[134] This Note seeks to flush out the contours of this restriction on the use of FISA materials and proposes a statutorily created means of enforcing the "inextricably intertwined" restriction analogous to FRE 104(a).

Minimizing the Use of Unrelated Evidence, 41 WAKE FOREST L. REV. 61, 103-09 (2006) (proposing that courts interpret the minimization requirement of the Fourth Amendment as limiting the use of FISA evidence to foreign intelligence prosecutions).

131. *See infra* notes 196–202.

132. *In re Sealed Case*, 310 F.3d at 736.

133. *Id.*

134. *Cf. supra* note 95 (listing all of those cases in which a court admitted FISA surveillance evidence in a non-foreign intelligence related prosecution); *supra* note 71 (listing many of the cases in which the court found the primary purpose of the surveillance to be the collection of foreign intelligence information).

A. The Easy Cases: Foreign Intelligence Crimes

Under an "inextricably intertwined" test, FISA evidence should clearly be admissible in the prosecution of foreign intelligence crimes including terrorism, espionage, and sabotage. In cases involving terrorism, FISA evidence would be admissible in prosecutions for hostage taking,[135] aircraft piracy,[136] possession or sale of an explosive or incendiary rocket or missile system designed to take down an airplane,[137] bombing a public or government space,[138] receiving military training from a terrorist organization,[139] possession or sale of biological weapons, chemical weapons, nuclear weapons and other weapons of mass destruction.[140] Espionage[141] and sabotage[142] crimes are also, in most cases, easily identifiable. The difficulty with the test, however, exists in distinguishing between ordinary prosecutions in which FISA evidence should not be admissible and those prosecutions in which FISA evidence should be admissible because the "ordinary crime" is actually "inextricably intertwined" with a foreign intelligence crime.

---

135. 18 U.S.C. § 1203 (2006).

136. 49 U.S.C. § 46502 (2000); *see also id.* § 46505 (criminalizing the carrying of a weapon or explosive on an aircraft); 18 U.S.C. § 32(b)(4) (2006) (criminalizing the destruction of aircrafts).

137. 18 U.S.C. § 2332g (2006); *see also id.* § 844(d) (criminalizing transportation or receipt of explosives with the knowledge or intent that it be used to kill, injure, or intimidate).

138. *Id.* § 2332(f).

139. *Id.* § 2339(d).

140. *Id.* §§ 2332(a) (criminalizing the use of weapons of mass destruction), 175 (criminalizing possession of biological weapons), 229 (making it illegal to use, produce, possess, or transfer a chemical weapon), 831 (criminalizing the possession of nuclear weapons), 832 (making it illegal to provide material support to a nuclear weapons program or other weapons of mass destruction program of a foreign terrorist power), 2332 (criminalizing possession of radiological dispersal devices).

141. *See, e.g., id.* §§ 792 (prohibiting the harboring or concealing of a person engaging in espionage), 793 (criminalizing the gathering, transmitting, copying or losing of defense information), 794 (criminalizing the gathering or delivering of defense information to aid foreign government), 795 (making it illegal to photograph or sketch defense installations), 796 (criminalizing the use of aircraft for photographing defense installations), 798 (prohibiting the disclosure of classified information); *see also id.* §§ 951 (criminal prohibition against acting as the agent of a foreign government), 953 (outlawing private correspondence with foreign governments), 954 (criminalizing the making of false statements intended to influence a foreign government to the injury of the United States), 957 (criminalizing the possession of property in aid of a foreign government).

142. *See* 18 U.S.C. §§ 2151–2156 (2006) (penalizing the sabotage or destruction of national defense facilities or materials); 42 U.S.C. § 2284 (2000) (penalizing the knowing sabotage of nuclear facilities).

B. Unrelated Cases in which the FISA Evidence Would be Excluded

A review of those cases in which courts have admitted FISA evidence of crimes should shed some light on the execution of this test. Of the sixty cases surveyed for this Note, a large majority would be unaffected by this proposed restriction. Many of the cases in which FISA materials have been introduced into evidence involve straightforward terrorism cases[143] or garden-variety espionage cases.[144] Other cases, however, involve the admission of FISA material in prosecutions for ordinary crimes that are only loosely connected or completely unrelated to a foreign intelligence crime. For example, in *United States v. Isa*, the government obtained a FISA warrant for surveillance of Zein Hassan Isa, a native-born Palestinian, who the FBI suspected of ties to the Palestinian Liberation

143. FISA evidence was admitted in the following terrorism prosecutions: United States v. Sarkissian, 841 F.2d 959, 965 (9th Cir. 1988) (convicting defendants, members of an Armenian terrorist organization, of conspiracy to bomb the Turkish Consulate in Philadelphia, transportation of explosive materials, and possession of an unregistered firearm after dynamite was discovered in their checked luggage); United States v. Hassoun, No. 04-60001-CR-COOKE/BROWN, 2007 WL 1068127, at *2–4 (S.D. Fla. Apr. 4, 2007) (defendants were charged with conspiracy to commit murder, maim, and kidnap people both in the U.S. and overseas); United States v. Jayyousi, No. 04-60001-CR-COOKE/BROWN, 2007 WL 851278 (S.D. Fla. Mar. 15, 2007) (trial of Hassoun's co-conspirator); United States v. Abu Ali, No. 05-053, 2006 WL 4483162 (E.D. Va. Feb. 17, 2006) (defendant was convicted of providing material support to al-Qaeda, conspiracy to assassinate the President, conspiracy to commit aircraft piracy, and conspiracy to destroy aircraft); United States v. Bin Laden, No. S7R 98CR1023KTD, 2005 WL 287404 (S.D.N.Y. Feb. 7, 2005) (defendants were convicted of conspiracy to murder U.S. nationals and to destroy U.S. buildings stemming from the 1998 synchronized attacks on the United States Embassies in Dar-es-Salaam, Tanzania and Nairobi, Kenya); United States v. Rahman, 861 F. Supp. 247, 249 (S.D.N.Y. 1994) (defendants were charged with "participating in a seditious conspiracy to conduct a war of urban terrorism against the United States"); United States v. Hovsepian, No. CR 82-917, 1985 WL 5970, at *3 (C.D. Cal. Jan. 15, 1985), *aff'd*, United States v. Berberian, 851 F.2d 236 (9th Cir. 1988) (defendant was convicted of conspiracy to bomb and aiding and abetting transportation of explosive material in connection with an attempt to blow up the Turkish Consulate in Philadelphia).

144. *See, e.g.*, United States v. Miller, 984 F.2d 1028, 1029–32 (9th Cir. 1993) (FISA material admitted in prosecution for selling classified information to the KGB); United States v. Pelton, 835 F.2d 1067, 1069–71, 1074–76 (4th Cir. 1987) (FISA surveillance used to catch an NSA defector to the Soviets. The defector was subsequently charged with espionage and unauthorized disclosure of classified information concerning communications intelligence); United States v. Cavanagh, 807 F.2d 787, 788–92 (9th Cir. 1987) (FISA evidence was admitted in prosecution of defendant for selling classified defense information to the Soviets); United States v. Ott, 637 F. Supp. 62, 63–67 (E.D. Cal. 1986), *aff'd*, 827 F.2d 473 (9th Cir. 1987) (serviceman unlawfully contacted representatives of foreign government to offer to sell them classified information); United States v. Nicholson, 955 F. Supp. 588, 592 (E.D. Va. 1997) (FISA materials admitted in espionage prosecution); United States v. Horton, 17 M.J. 1131, 1132–34 (N-M Ct. Rev. 1984) (defendant was convicted in Navy Court of failing to report contacts with citizens of a communist controlled country and soliciting sale of classified information).

Organization.[145] During the FBI's surveillance of Isa, they overheard Isa and his wife, Maria Matias Isa, murder their sixteen-year-old daughter. Prosecutors later introduced tapes of the murder, as well as conversations surrounding it, during the trial of Isa and his wife for first degree murder.[146] Despite the tragic factual circumstances of this case, the actual tapes of the murder should have been excluded because the murder was completely unrelated to foreign intelligence or national security. The government would still be free to use the fruits of this surveillance to prosecute Isa and his wife for murder on the basis of other independently obtained evidence.[147] In *U.S. v. Brown*, the government obtained a FISA warrant to surveil several suspected agents of the Libyan government.[148] Pursuant to this warrant, the government wiretapped the phone of the Manara Travel Agency,[149] and inadvertently stumbled upon a conspiracy to commit credit card fraud using stolen calling card access numbers involving people who were not the targets of the surveillance. This case represents a fairly common scenario in which the government discovers criminal activity through the inadvertent interception of the communications of someone other than the "foreign agent" targeted by the FISA wiretap.[150] Under the "inextricably intertwined" test proposed in this Note, the FISA evidence would be excluded at a later trial because the credit card fraud is unrelated to a foreign intelligence crime.[151]

145. United States v. Isa, 923 F.2d 1300 (8th Cir. 1991).

146. *Id.* at 1302.

147. Both the "inevitable discovery rule" and the "independent source" doctrine would still, of course, apply and evidence of a non-foreign intelligence crime could still be admitted under either of those methods of dissipating the taint. The inevitable discovery rule allows the admission of unconstitutionally seized evidence that would have inevitably been discovered through lawful means. *See* Nix v. Williams, 467 U.S. 431, 443 (1984); *see also* Martin J. McMahon, *What Circumstances Fall within "Inevitable Discovery" Exception to Rule Precluding Admission, in Criminal Case, of Evidence Obtained in Violation of Federal Constitution*, 81 A.L.R. FED. 331 (1987). The "independent source" doctrine permits the introduction of evidence initially discovered during, or as consequence of, an unlawful search, but later rediscovered independently through lawful means untainted by the initial illegality. *See, e.g.*, Murray v. United States, 487 U.S. 533, 537–39 (1988) (describing the origin and contours of the independent source doctrine). In addition, there is a powerful argument that these rules should be applied liberally in the context of FISA evidence because the police have not necessarily acted illegally.

148. 908 F.2d 968 (Table), Nos. 89-5404 to 89-5407, 1990 WL 101946, at *1 (4th Cir. June 21, 1990).

149. *Id.*

150. *See infra* note 183.

151. Any exculpatory evidence generated through the FISA surveillance should still clearly be admissible in a prosecution of a non-foreign intelligence crime. Although, the prosecution is not required to comb through the FISA surveillance for exculpatory evidence. *See supra* note 35.

C. Borderline Cases: Crimes Committed to Provide Material Support to a FTO

The situation posing the greatest difficulty for the "inextricably intertwined" test is one in which the target of FISA surveillance commits an ordinary crime allegedly to raise money or provide "material support" to a foreign terrorist organization ("FTO").[152] There are powerful policy arguments in favor of admitting FISA material in these cases if the government can establish a sufficient nexus to terrorism or espionage. On the other hand, the restriction becomes meaningless if the government can circumvent it simply by alleging a link to terrorist activities. The government should be required to prove some connection with a foreign intelligence crime or activity in order to reap the benefits of FISA surveillance.

This Note proposes a two-step process in prosecutions for ordinary crimes allegedly linked to a foreign intelligence crime. First, the government must charge the defendant with a foreign intelligence crime or with material support of a terrorist organization. An indictment requires the government to demonstrate probable cause supporting the charge that the defendant committed either a foreign intelligence crime or an ordinary crime in order to support a terrorist organization. Second, the judge will review the government's proof *in camera* and, if the judge finds by a preponderance of the evidence[153] that the ordinary crime is "inextricably intertwined" with the foreign intelligence crime, then the FISA evidence should be admitted in the criminal trial.[154]

The large majority of "material support" cases, involving the direct sale of arms to a terrorist group[155] or the laundering of money

152. *See supra* note 7.

153. A clear and convincing standard of proof might also be appropriate.

154. Under Federal Rules of Evidence 104(a) and (b), a procedure already exists for determining preliminary questions regarding the admissibility of evidence. FED. R. EVID. 104(a)-(b). For example, a trial judge must find by a preponderance of evidence that the statement of a co-conspirator was (1) made during the course and (2) in furtherance of the conspiracy to justify its introduction into evidence against the defendant. FED. R. EVID. 104(b). In making its determination regarding the admissibility of this evidence, the court is not bound by the rules of evidence. FED. R. EVID. 104(a).

155. FISA evidence was admitted in the following cases involving the smuggling of weapons or arms to a terrorist organization: United States v. McKinley, 995 F.2d 1020, 1022–24 (11th Cir. 1993) (admitting FISA evidence in prosecution of defendant for sale of stinger missiles and other explosives to the IRA and conspiracy to blow up a British airliner); United States v. Badia, 827 F.2d 1458, 1460–64 (11th Cir. 1987) (admitting FISA evidence against a defendant charged with selling weapons to his co-defendant, who is a member of Omega-7, a militant anti-Castro group); United States v. Megahey, 553 F. Supp. 1180, 1182 (E.D.N.Y. 1982), *aff'd*, United States v. Duggan, 743 F.2d 59 (2d Cir. 1984) (defendants were convicted, in part from FISA evidence, of unlicensed exportation of items on the United States Muni-

to a terrorist group,[156] will easily satisfy the "inextricably intertwined" test. Similarly, most espionage prosecutions involve a defendant selling state secrets, military technology, or classified materials directly to a foreign agent. As a result, the government should have no trouble meeting the standard of proof necessary to admit the FISA material.[157]

The government has, however, utilized FISA evidence in several "ordinary" prosecutions without demonstrating probable cause to believe that the defendant is linked to a terrorist organization. In

---

tions List, various firearm offenses and transportation of explosives in interstate commerce knowing that the explosives would be used to kill, injure, or intimidate individuals); United States v. Falvey, 540 F. Supp. 1306, 1313–14 (E.D.N.Y. 1982) (admitting FISA evidence in a prosecution for smuggling arms and equipment to the Provisional Irish Republican Army).

156. FISA evidence was admitted in the following cases involving charges of providing material support to a terrorist organization: United States v. Hammoud, 381 F.3d 316, 325–26 (4th Cir. 2004) (defendant was convicted, pursuant to FISA evidence, of providing material support to a designated foreign terrorist organization, along with possibly related crimes, including money laundering, credit card fraud, and transportation of contraband cigarettes); United States v. Holy Land Found. for Relief and Dev., No. 3:04-CR-240-G, 2007 WL 2011319, at *1–2 (N.D. Tex. Jul. 11, 2007) (prosecution for donations to various organizations affiliated or controlled by Hamas, an FTO); United States v. Warsame, No. 04-29 (JRT), 2007 WL 748281, at *1 (D. Minn. Mar. 8, 2007) (defendant was convicted of providing material support and resources to a Foreign Terrorist Organization); United States v. Abdi, 498 F. Supp. 2d 1048, 1051–52 (S.D. Ohio 2007) (FISA evidence admitted in prosecution of defendant for providing material support to al-Qaeda and receiving military training in preparation for violent Jihad in Ogaden, Ethiopia); United States v. Assi, 414 F. Supp. 2d 707, 709–11 (E.D. Mich. 2006) (defendant was charged with providing technical equipment to Hezbollah including two Boeing global positioning satellite modules, night vision goggles, and a thermal imaging camera); United States v. Elashi, 440 F. Supp. 2d 536, 541–43 (N.D. Tex. 2006) (admitting FISA evidence in prosecution of defendants for laundering money in order to provide material support to Hamas, an FTO); United States v. Al-Arian, 267 F. Supp. 2d 1258, 1259–60 (M.D. Fla. 2003) (members of the University of South Florida faculty charged with providing material support in the form of money to the Palestinian Islamic Jihad Shiqaqi Faction (PIJ) and succor to the families of suicide bombers).

157. The following cases, which involve the admission of FISA evidence in espionage prosecutions, would probably also proceed unaffected by the implementation of the "inextricably intertwined" test: United States v. Wen, 477 F.3d 896, 897 (7th Cir. 2007) (defendants found guilty of violating export-control laws by providing militantly useful technology to foreign country without required license); United States v. Campa, 459 F.3d 1121, 1126–27 (11th Cir. 2006) (admitting FISA evidence in prosecution of defendants for serving as agents of the Cuban government and transmitting secret intelligence information to the Cuban government); United States v. Squillacote, 221 F.3d 542, 547–52 (4th Cir. 2000) (husband and wife were convicted of conspiracy to transmit information relating to the national defense); United States v. Posey, 864 F.2d 1487, 1489–90 (9th Cir. 1989) (admitting evidence in prosecution of defendant for selling military technology to the South African government in violation of the Anti-Apartheid Act); United States v. Thomas, No. 06 CR. 365(DLC), 2006 WL 2283772, at *1 (S.D.N.Y. Aug. 9, 2006) (defendant was convicted for selling telecommunications equipment to the Iraqi government through China due in part to the admission of FISA evidence); United States v. Rosen, 447 F. Supp. 2d 538, 541–42 (E.D. Va. 2006) (admitting FISA evidence in prosecution for conspiring to communicate national defense information to persons not entitled to receive it); United States v. Dumeisi, No. Civ.A. 06C4165, 2006 WL 2990436, at *1–2 (N.D. Ill. Oct. 17, 2006) (Defendant Khaled Abded-Latif Dumeisi was convicted of acting as an agent of Iraq).

United States v. Jamal, for example, the government indicted Jamal and several others entangled in a large fencing operation which involved stealing or fraudulently obtaining baby formula and transporting it across state lines to make a large profit.[158] The defendants made over eleven million dollars, which they allegedly funneled to sources in Syria and Lebanon.[159] The government, however, never offered any evidence connecting the defendants with any terrorist group and for some reason did not charge the defendants with material support of a terrorist organization.[160] Unless the government could muster some proof of a connection to a foreign intelligence crime, under the test proposed herein, the FISA materials would be inadmissible against the defendants. Similarly, in *United States v. Mubayyid*, the defendants were prosecuted for making false statements on their tax returns and fraudulently obtaining a charitable exemption for their organization, Care International ("Care").[161] Care allegedly solicited funds for, and issued publications promoting, Islamic holy war, or "jihad."[162] Based on the limited opinion released to the public, the government provided no evidence of the connection between Mubayyid and any terrorist organization and opted not to charge the defendants with material support of any terrorist organization.[163] Under the proposed test, the government, in these two cases, might not be able to meet the standard of proof necessary for the admission of the FISA evidence because it apparently lacked sufficient evidence to convict the defendants of providing material support to a terrorist organization.

Since September 11th, the government has increasingly used perjury prosecutions and deportation proceedings as a way to in-

158. United States v. Jamal (Jamal I), 285 F. Supp. 2d 1221, 1222–24 (D. Ariz. 2003), *aff'd*, United States v. Daly, Nos. 05-10718, 05-10719, 05-10728, 05-10729, 243 F. App'x 302, 306 (9th Cir. 2007); *see also* Joseph A. Reaves, *Fourteen Arrested in Alleged Money-Laundering Operation in Southern Florida*, THE ARIZONA REPUBLIC, Aug. 1, 2003, at A1, *available at* http://www.policeone.com/investigations/articles/66262/.

159. *Jamal I*, 285 F. Supp. 2d at 1222.

160. The defendants were charged with "eight (8) felonies: Conspiracy to Commit Interstate Transportation of Stolen Property (Count 1); Interstate Transportation of Stolen Property (Counts 2, 3 and 4); False Statements (Counts 5, 6 and 7); and Conspiracy to Commit Money Laundering." Jamal I, 285 F. Supp. 2d at 1222; *see* Reaves, *supra* note 158, at A1 ("Authorities, however, avoided linking any of those arrested with terrorist activities. 'We want to make sure that the individuals who are charged in this case defend themselves on the counts they are charged with and not on speculation or hypotheticals,' said U.S. Attorney Paul K. Charlton, who announced the crackdown.").

161. United States v. Mubayyid, No. 05-40026-FDS, 2007 WL 3287393, at *1 (D. Mass. Nov. 5, 2007).

162. *Id.*

163. *Id.* The defendants were charged with conspiracy to defraud the United States, false statements, and obstructing and impeding the Internal Revenue Service.

capacitate suspected terrorists.[164] If the government lacks sufficient evidence in these cases to bring a material support charge then, under the "inextricably intertwined" test, the government would be precluded from admitting FISA evidence to prove the falsity of a defendant's claim that he is not a member or supporter of a terrorist organization. For example, in *U.S. v. Benevolence Intern Foundation, Inc.*, the government presented FISA evidence to charge the CEO of the Benevolence International Foundation ("BIF") with perjury for claiming: "BIF has never provided aid or support to people or organizations known to be engaged in violence, terrorist activities, or military operations of any nature."[165] Yet, for some reason, the government never charged BIF or its CEO with providing material support to an FTO even after the perjury indictment was subsequently dismissed. If this decision not to proceed with a material support prosecution was due to a lack of evidence, then under the inextricably intertwined test this FISA evidence would be inadmissible in the perjury prosecution.[166]

---

164. According to an ICE spokesman, Dean Boyd, from 2003–2005, officials filed immigration charges against more than 500 people who have come under scrutiny in national security investigations. Many of these 500 people were ultimately found to have no terrorism ties. "Homeland Security officials say immigration laws can provide a quick, easy way to detain people who could be planning attacks. Authorities have also used routine charges such as overstaying a visa to deport suspected supporters of terrorist groups." Mary Beth Sheridan, *Immigration Law as Anti-Terrorism Tool*, WASH. POST, June 13, 2005, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/06/12/AR2005061201441.html; *see also* Homeland Security Presidential Directive 2: Combating Terrorism Through Immigration Policies, Oct. 29, 2001, http://www.whitehouse.gov/news/releases/2001/10/20011030-2.html (establishing the "Foreign Terrorist Tracking Task Force" to locate, detain, prosecute, or deport any aliens associated with terrorist organizations who are already present in the United States).

165. No. 02 CR 414, 2002 WL 31050156, at *7 (N.D. Ill. Sept. 13, 2002); *see also* United States v. Damrah, 412 F.3d 618, 620–22 (6th Cir. 2005) (admitting FISA evidence in prosecution for unlawfully obtaining citizenship by making false statements denying involvement with the Palestinian Islamic Jihad); *In re* Grand Jury Proceedings of Special April 2002 Grand Jury, 347 F.3d 197, 204–06 (7th Cir. 2003) (holding witness in contempt for refusing to answer grand jury questions and rejecting witnesses' argument that he should not be required to answer questions based upon an allegedly unconstitutional FISA wiretap); *In re* Grand Jury Proceeding, Grand Jury No. 87-4 Empaneled, 856 F.2d 685, 687–90 (4th Cir. 1988) (using FISA material to formulate questions in a grand jury proceeding).

166. One potential complication arises in prosecutions in which the underlying "material support" or foreign intelligence counts are dismissed after the FISA evidence has been introduced in the trial of the "inextricably intertwined" non-foreign intelligence crime. If the grand jury found probable cause for the material support charge and the judge found a sufficient nexus between the material support crime and the "ordinary crime" then the evidence should still be admissible in these types of situations and a dismissal (or failure to convict) of the other counts should not constitute reversible error. *See, e.g.*, United States v. Benkahla, 437 F. Supp. 2d 541 (E.D. Va. 2006) (the defendant was prosecuted for making false statements to a grand jury regarding a trip that he took to Pakistan in 1999 during which the government alleges that he received military training from the Taliban. The defendant was initially charged with "willfully supplying and attempting to supply services" to a

Finally, deportation proceedings present a rare exception to the rule, proposed herein, that the government should not be allowed to admit FISA evidence when it lacks sufficient evidence to prove a link to a foreign intelligence crime. Any type of evidence, including hearsay,[167] illegally seized evidence,[168] and character evidence, is admissible in a deportation proceeding and a failure to demonstrate "good character" can disqualify an applicant for citizenship.[169] In addition, given that the individual interest at stake in an immigration proceeding is less than that at stake in a criminal proceeding, there is a powerful policy argument that FISA evidence should be admissible.

V. ARGUMENTS FOR THE INEXTRICABLY INTERTWINED TEST

The inextricably intertwined test reestablishes the proper balance between individual rights and the state interest in national

---

foreign terrorist organization, Lashkar-e-Taiba ("LET"), in violation of 50 U.S.C. § 1705 (2000). However, LET had not yet been designated a FTO at the time and consequently, the charges were dismissed. As a result, this presents another situation in which under the "inextricably intertwined" test, the FISA material should be excluded); *see also* United States v. Sattar, 272 F. Supp. 2d 348, 356–61 (S.D.N.Y. 2003) (dismissing the counts related to "providing material support" to a terrorist organization as unconstitutionally vague. Under the "inextricably intertwined test" proposed herein, if these counts were dismissed then it would probably necessitate the exclusion of the FISA evidence in the underlying criminal prosecution); United States v. Sattar, No. 02 CR 395, 2003 WL 22137012, at *1 (S.D.N.Y. Sept. 15, 2003).

167. *See* Ernest H. Schopler, *Hearsay Evidence in Proceedings before Federal Administrative Agencies*, 6 A.L.R. FED. 76 § 12[b] (2007) ("Notwithstanding a decision of the United States Supreme Court reaching a contrary result under the circumstances presented, the lower federal courts seem to agree that in administrative deportation proceedings, evidence should not be excluded merely because of its nature as hearsay.").

168. The case law is divided on this point with some circuits admitting illegally seized evidence in deportation proceedings and others only admitting the fruits of an illegal search. Daniel E. Feld, *Admissibility, in Deportation Hearing, of Evidence Obtained by Illegal Search and Seizure*, 44 A.L.R. FED. 933 (2007).

169. The Nationality Act of 1940 provides: "[n]o person . . . shall be naturalized unless such petitioner, . . . during all the periods referred to in this subsection has been and still is a person of good moral character." 8 U.S.C. § 707(a)(3) (2006). Whether a particular applicant evinces good moral character is a question of fact. *See, e.g.*, Daddona v. United States, 170 F.2d 964, 966 (2d Cir. 1948). The burden of proving good moral character is typically placed on the applicant, with any doubts to be resolved against him or her. *In re* Kovacs, 476 F.2d 843, 845 (2d Cir. 1973); Nemetz v. I.N.S., 647 F.2d 432, 435 (4th Cir. 1981). Hearsay regarding the applicant's general reputation in a community is also often deemed admissible. Petition of B., 154 F. Supp. 633, 634 (D. Md. 1957). *See generally* 3C AM JUR 2D. ALIENS § 2312 (2007). Participation in, or support of, terrorist activities has been held to require deportation of an alien and the Patriot Act, Pub L. 107-56, § 411, 345–50, expanded the grounds for deportation to include "terrorist related" activities. 8 U.S.C. § 1182(a)(3)(B)(iii)(V)(b) (2006); *see also* McAllister v. Attorney General of U.S., 444 F.3d 178 (3d Cir. 2006), *cert. denied*, 127 S. Ct. 667 (U.S. 2006) (deporting an alien on the grounds that he had engaged in terrorist activities).

security that was sacrificed in the Patriot Act. This test also addresses the central concerns identified by critics of the significant purpose test and gives the judiciary an important role in checking the executive's use of its surveillance powers. First, by preventing the use of FISA materials in ordinary prosecutions that do not have a link to foreign intelligence crimes, this test deters law enforcement personnel from pretextually seeking a FISA warrant in a case involving only ordinary criminal activity. A law enforcement agent would have no reason to seek a FISA warrant unless he suspected the target of engaging in a foreign intelligence crime. Second, the inextricably intertwined test will, to a certain extent, decrease the disproportionate enforcement of "ordinary laws" against Muslims, Arab Americans, and other groups. These minority groups may still be disproportionately targeted by FISA applications but at least they will not be subjected to a lesser standard of Fourth Amendment protection in non-foreign intelligence prosecutions. Third, this restriction will deter the use of FISA warrants to gather evidence to prosecute political opponents and persons who engage in disfavored speech. Finally, by preventing the introduction of FISA evidence at the trial of a person whose communications have been incidentally intercepted by a FISA warrant, this test would eliminate the unjust forfeiture of a person's Fourth Amendment protections that results simply by associating with a FISA target or using the same phone line or trunk line as a FISA target.

At the same time, a restriction on the use of FISA materials avoids the difficulties involved in drawing a line based on the subjective intent of the officers involved in the surveillance.[170] Moreover, by refusing to resurrect the "primary purpose wall," the "inextricably intertwined test" allows intelligence personnel to communicate, cooperate, and share information without the fear of jeopardizing a future prosecution. The amorphous nature of terrorist plots and the difficulty of infiltrating a variety of disconnected terrorist cells necessitate the cooperation of different intelligence branches. This test allows intelligence personnel to keep tabs on suspected terrorists and other national security threats without demonstrating probable cause, thereby enabling the marshaling of the government's resources toward preventing another catastrophic attack.

170. Indeed, the difficulty of determining the subjective intent of officers involved in a search has led courts to shy away from this criterion in a variety of contexts. *See, e.g.*, Whren v. United States, 517 U.S. 806, 813 (1996) (holding that the constitutional reasonableness of a traffic stop does not depend on the motivations of the individual officers involved); *see also* Horton v. California, 496 U.S. 128 (1990) (eliminating the subjective requirement, in a plain view context, that officers "inadvertently discover" evidence).

Moreover, as the war on terrorism progresses it is important that as a society we encourage our government to combat terrorism within the confines of the legal system. The Bush administration has employed a series of extra-legal methods including torture, the detention of enemy combatants without habeas review, and the implementation of the Terrorist Surveillance Program ("TSP").[171] It has justified these tactics by arguing that the legal system in its current form does not provide effective tools for fighting terrorism.[172] By enabling intelligence officers to cooperate with each other and then bring foreign intelligence prosecutions, the inextricably intertwined test is superior to the primary purpose test because it brings terrorists within the confines of the criminal justice system. By contrast, if the primary purpose test were resurrected and government officials feared FISA evidence would be excluded, then intelligence officials might indefinitely detain a suspect at a black site[173] instead of risking an unsuccessful prosecution. In a similar vein, David Kris has argued that the fall of the primary purpose wall will actually

171. Evidence exists that various government agencies continue to engage in extra-legal surveillance and data-mining without any oversight. *See* Bradley Olson, *Domestic Spying Quietly Goes On*, BALTIMORE SUN, Jul. 7, 2008, at A.1.

172. *See infra* text accompanying notes 205–06; *see also* Press Release, Alberto R. Gonzales, Attorney Gen., and Gen. Michael Hayden, Principal Deputy Dir. for Nat'l Intelligence (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html (Gen. Michael Hayden, discussing how the "agility" of the TSA allowed the NSA to track terrorist cells, stated, "I can say unequivocally, all right, that we have got information through this program that would not otherwise have been available [under FISA]."); James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html (The eavesdropping program grew out of concerns after the Sept. 11 attacks that the nation's intelligence agencies were not poised to deal effectively with the new threat of Al Qaeda and that they were handcuffed by legal and bureaucratic restrictions better suited to peacetime than war, according to officials.); John Ashcroft, Attorney Gen., Testimony Before the House Committee on the Judiciary (Sept. 24, 2001), *available at* http://www.usdoj.gov/ag/testimony/2001/agcrisisremarks9_24.htm ("Law enforcement tools created decades ago were crafted for rotary telephone—not email, the Internet, mobile communications, and voice mail. Every day that passes with outdated statutes and the old rules of engagement—each day that so passes is a day that terrorists have a competitive advantage."). *See generally* Jane Mayer, *Outsourcing Torture*, THE NEW YORKER, Feb. 14, 2005, at 106, *available at* http://www.newyorker.com/printables/fact/050214fa_fact6 (discussing the "extraordinary rendition" program and the Bush administration's justifications for the program).

173. In military terminology, a black site is a location at which a black project (a secret project unacknowledged by the U.S. government) is conducted. In the context of the war on terror, the term black site has come to refer to secret CIA prisons outside of the United States used to hold enemy combatants with little or no political oversight. Various commentators have hypothesized that these prisons are situated in countries that tolerate torture. *See* Dafna Linzer & Julie Tate, *New Light Shed on CIA's Black Sites*, WASH. POST, Feb. 28, 2007, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/02/27/AR2007022702214_pf.html; *Bush Admits CIA Black Sites*, SPIEGEL ONLINE INT'L, Sept. 5, 2006, http://www.spiegel.de/international/0,1518,435736,00.html.

increase the protection of civil liberties under FISA by increasing the involvement of Department of Justice ("DOJ") lawyers in intelligence investigations.[174]

Finally, the constitutional arguments in favor of a foreign intelligence exception to the Fourth Amendment, namely the "special need" of the government to protect national security and the President's Article II power,[175] recede into the background in the context of non-foreign intelligence prosecutions.[176] Therefore, by confining the use of FISA material to foreign intelligence prosecutions, this test solidifies the shaky constitutional ground on which FISA, as amended by the Patriot Act, currently rests.[177]

VI. AN ARGUMENT AGAINST THE INEXTRICABLY INTERTWINED TEST

This Part aims to dispel the most common criticism of the restriction proposed by this Note—that the inextricably intertwined test violates the plain view doctrine.[178] While it is undoubtedly true that this test would result in the exclusion of "plain view" evidence of some non-foreign intelligence crimes, the policy rationale underlying the plain view doctrine is inapplicable to electronic communications gathered under FISA.

Electronic surveillance invades a much wider realm of privacy rights than a normal physical search; electronic surveillance exposes every email, fax, text message, phone conversation, and

174. David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487, 523–24 (2006) (according to Kris, the FISA wall kept DOJ lawyers in the field completely separated from intelligence investigations whereas after the *In re Sealed Case* decision, prosecutors will "control and direct" intelligence investigations. Kris argues that the orientation of DOJ lawyers toward preserving the option of criminal prosecution makes them especially sensitive to preventing violations of individual rights that could affect the subsequent criminal case).

175. *See* Sullivan, *supra* note 53, at 402–12 (presenting the aforementioned arguments in favor of FISA's constitutionality).

176. *See* United States v. Truong, 629 F.2d 908, 915 (4th Cir. 1980) (justifying the primary purpose test by arguing that "once surveillance becomes primarily a criminal investigation . . . individual privacy interests come to the fore and government foreign policy concerns recede").

177. *See* Mayfield v. United States, 504 F. Supp. 2d 1023, 1036–42 (D. Or. 2007) (holding that the Foreign Intelligence Surveillance Act as amended by the Patriot Act is unconstitutional).

178. *See generally* United States v. Isa, 923 F.2d 1300, 1304–05 (8th Cir. 1991) ("If Federal agents monitoring a foreign intelligence surveillance authorized under this chapter were to overhear information relating to a violation of State criminal law, such as homicide, the agents could hardly be expected to conceal such information from the appropriate local officials.").

movement that a target makes.[179] Indeed, the nature of electronic communications makes it impossible to determine the destination or source of an email sent along a network's trunk line without decoding and reading the entire email.[180] This aspect of email communications makes it impossible to "minimize"[181] the acquisition and dissemination of (1) personal emails unrelated to the target's criminal activity and (2) emails of other people using the same trunk line.[182] The "incidental" interception of the communications of anyone using the same trunk line as a suspect creates a potentially gigantic hole in Fourth Amendment protections by allowing the government to wiretap a large group of people without ever demonstrating probable cause regarding those people.[183] In many cases, a warrant issued for one person would necessitate the review of a large number of emails involving the personal communications of other unrelated people.[184] Therefore, electronic

179. *See supra* notes 125–26.

180. *See* Larry Downes, *Electronic Communications and the Plain View Exception: More "Bad Physics,"* 7 HARV. J.L. & TECH. 239, 265 (1994) [hereinafter Downes] ("For digital communications, however, it is impossible to determine the nature of the communication using the traditional minimization technique, because several layers of hardware and software must be applied to convert the intercepted signal, first to its digital format, then to a recognizable communications protocol, and finally to a format understandable to human beings. The sender, receiver, and subject of a message are unknown until the last step. It is impossible to discard a digital communication that is unrelated to the subject offenses until after all of its contents are revealed to the investigators."); *see also* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 611–22 (2003) (describing the pre-internet Fourth Amendment distinction between the address information on the outside of the envelope and the content contained within the envelope as outdated when applied to the internet because of the impossibility of disentangling the envelope information, i.e., the IP address, from the content of the email).

181. Berger v. New York, 388 U.S. 41, 58–60 (1967) (declaring a New York statute unconstitutional because it failed to prevent indiscriminate wiretapping). *See, e.g.*, Bynum v. United States, 423 U.S. 952, 952–53 (1975) (explaining that the minimization provision in Title III which requires that every intercept be conducted in such a way as to minimize the interception of unrelated communications "constitutes the congressionally designed bulwark" designed to adhere to the constitutional guidelines announced in *Berger*).

182. The "truck line" is the line of communication between the telecommunications carrier and a network of phones, computers, and fax machines.

183. Indeed, the incidental interception of an incriminating phone call has already led to several convictions. *See, e.g.*, United States v. Johnson, 952 F.2d 565, 570 (1st Cir. 1991); United States v. Badia, 827 F.2d 1458, 1461 (11th Cir. 1987); United States v. Cavanagh, 807 F.2d 787, 788–89 (9th Cir. 1987); United States v. Duggan, 743 F.2d 59, 79 (2d. Cir. 1984); United States v. Sattar, No. 02 CR. 395(JGK), 2003 WL 21698266, at *2 (S.D.N.Y. Jul. 22, 2003); United States v. Rahman, 861 F. Supp. 247, 252 (S.D.N.Y. 1994); United States v. Belfield, 692 F.2d 141, 143 (D.C. Cir. 1982). This problem will only become worse with the increased use of digital communications and the internet.

184. For example, many offices and businesses utilize private branch exchanges (PBXs) to connect their faxes, telephones and internet to the outside telecommunications carrier. In order to intercept the communications of one person within the office or business, the government would have to place the wiretap on the trunk line and intercept all communications going to and from the office building. The government would then decode these

communications not only invade the privacy rights of the individual to a greater degree than a normal search[185] but they also infringe on the privacy rights of a greater number of innocent persons.

At the same time, the limitations placed on the plain view doctrine in the context of physical searches do not protect individual rights when applied to electronic surveillance. Police may constitutionally seize evidence in plain view only when (1) the seizing officer is lawfully in place to make the seizure and the "scope" of the search is reasonable; (2) it is immediately apparent[186] to the officer that the seized item constitutes evidence; and (3) the discovery of the evidence in plain view is inadvertent.[187] As with the primary purpose test, courts have largely eliminated the third requirement due to the difficulty of determining the officer's subjective intent.[188] As a result, the "immediately apparent" requirement and the scope limitation[189] on the plain view doctrine have gained increasing relevance as a means of preventing the police from engaging in pretextual searches.[190]

---

transmissions, retaining those involving criminal activity and discarding those unrelated to criminal activity. *See* Downes, *supra* note 180, at 239, 264 (posing the example of a Title III warrant issued for a broker suspected of insider trading at a large brokerage firm and stating that "[t]apping the trunk line captures all communications, analog and digital, transmitted to and from the office under investigation"); *see also* Kerr, *supra* note 180, at 650 (analogizing the government's surveillance of internet communications to a police officer walking through a crowd; surveilling a suspect necessitates scanning "all of the traffic flowing over the network to locate, isolate, and collect the IP headers.").

185. United States v. Cox, 449 F.2d 679, 686 (10th Cir. 1971) *cert. denied*, 406 U.S. 934 (1972) (stating that "the search for property is a different and less traumatic invasion than is the quest for private conversations").

186. "Immediately apparent" means that the police officer has probable cause to believe that the item in plain view is incriminating in nature. *See, e.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971) (stating 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.").

187. *Id.*

188. *See* Horton v. California, 496 U.S. 128, 138–40 (1990).

189. If the warrant specifies a large object, then the police cannot search in places unable to contain an object of that size. *See id.* at 141–42 (upholding the admission of the guns used to commit the robbery discovered in "plain view" while searching for the proceeds of the robbery (rings)).

190. *Id.* at 139–40 (dismissing the "inadvertent discovery" requirement because society's interest in "prevent[ing] the police from conducting general searches, or from converting specific warrants into general warrants, is not persuasive because that interest is already served by the requirements that no warrant issue unless it 'particularly describ[es] the place to be searched and the persons or things to be seized,'" and that "[s]crupulous adherence to these requirements serves the interests in limiting the area and duration of the search that the inadvertence requirement inadequately protects").

The realities of electronic surveillance are such that neither of these limitations is particularly effective in this context. First, under the plain view doctrine, police cannot look in places unlikely to contain the objects specified in the warrant[191] or manipulate an object in order to find evidence.[192] In the context of electronic communications, the criminal nature of the evidence is never "immediately apparent" and digital signals sending emails, faxes, and phone calls must be "manipulated" (translated from digital code to English) in order to be understood.[193] Second, as discussed above, the decoding process makes minimizing the acquisition of unrelated digital signals almost impossible; a computer recording a digital signal cannot stop listening when the conversation becomes impertinent.

A recognition of these concerns led several courts[194] and commentators[195] to question the applicability of the plain view doctrine to the interception of electronic communications under Title III. Indeed, in order to protect constitutional rights, Title III imposes additional procedural prerequisites for the admissibility of electronically-intercepted plain view evidence.[196] Under § 2517(5) of

191. *Id.*

192. *See* Minnesota v. Dickerson, 508 U.S. 365, 377–79 (1993) (excluding the evidence because its incriminating nature was not "immediately apparent"; the officer had to squeeze, slide, and manipulate the small object before he realized that it was crack cocaine); Arizona v. Hicks, 480 U.S. 321, 324 (1987) (excluding stolen turntables discovered at the defendant's house because the officer had to move the turntables to find their serial numbers and then run those serial numbers through a police database and therefore the criminal nature of the turntables was not immediately apparent).

193. *See* Downes, *supra* note 180, at 241 n.9 ("The modern approach, however, invariably includes converting the communication to a digital signal, which must be decoded by sophisticated software to be 'understood' on the receiving end. Image and data are often encrypted, and in any event are never sent in forms that are meaningful without interpretation by additional software—often proprietary to the receiver or the carrier. Introduction of 'wiretap' evidence may increasingly require expert witnesses to explain the government's translation processes and technologies.").

194. *See* John D. LaDue, *Electronic Surveillance and Conversations in Plain View: Admitting Intercepted communications Relating to Crimes Not Specified in the surveillance Order*, 65 NOTRE DAME L. REV. 490, 491 n.13 (1990) [hereinafter LaDue] (citing United States v. Williams, 737 F.2d 594, 605 (7th Cir. 1984) and United States v. Cox, 449 F.2d 679, 686 (10th Cir.), *cert. denied*, 406 U.S. 934 (1971)).

195. *Compare* Downes *supra* note 180, *and* Raymond R. Kepner, *Subsequent Use of Electronic Surveillance Interceptions and the Plain View Doctrine: Fourth Amendment Limitations on the Omnibus Crime Control Act*, 9 U. MICH. J.L. REF. 529, 540–53 (1976), *with* LaDue, *supra* note 194, at 526–33 (arguing that procedural safeguards to the use of plain view evidence obtained pursuant to a Title III wiretap should be removed). *See also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (arguing that the plain view doctrine should not apply in the context of searches of computer hard-drives).

196. Under 18 U.S.C. § 2517(5) (2006), plain view evidence is only admissible if "a judge of competent jurisdiction . . . finds on *subsequent application* that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable" (emphasis added). The legislative history explains that

Title III, evidence of other crimes, not listed in the application, is admissible only if an amendment to the original application is accepted by a judge who finds: (1) the original order was properly obtained; (2) the original order was not sought pretextually as a "subterfuge search" for evidence of the unlisted crime; and (3) the application for the amendment was made as soon as practical.[197] The second requirement appears intended to prevent police officers from using evidence that they did not "inadvertently discover," thereby deterring the pretextual use of § 2517(5). Moreover, thirty-two state statutes impose additional restrictions on the use of plain view evidence obtained pursuant to Title III.[198] In Nevada[199] and Connecticut,[200] for example, the surveillance evidence is inadmissible but the officers may use fruits of the illegal surveillance. In comparison, California's statute bars the use of both unauthorized intercepted communications concerning crimes not specified in the original order and fruits derived from the unauthorized intercept.[201] Finally, several states limit the admission of plain view evidence to prosecutions of certain enumerated felonies.[202] Interestingly, Title III and many state statutes have crafted an exception to their procedural requirements for the admission of "plain view" evidence in cases involving (1) an offense "similar to" the underlying offense; or (2) an offense that is an "integral part" of the crime specified in the underlying application.[203] Title III and these state

---

this plain view evidence may only be admitted in a subsequent judicial proceeding upon a showing that "the original order was lawfully obtained, that it sought in good faith and not as a subterfuge search, and that the communication was in fact incidentally intercepted during the course of a lawfully executed order." S. REP. No. 90-1097, at 100 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2180, 2189.

197. 18 U.S.C. § 2517(5) (2006).

198. LaDue, *supra* note 194, at 521 n.190.

199. NEV. REV. STAT. ANN. § 179.465(4) (West 2008).

200. CONN. GEN. STAT. ANN. § 54-41p(c), (d) (West 2008).

201. CAL. PENAL CODE § 629.32(b) (West 2007).

202. *See, e.g.*, COLO. REV. STAT. ANN. § 16-15-102(16) (West 2008); FLA. STAT. ANN. § 934.08(5) (West 2002); GA. CODE ANN. § 16-11-64(c) (West 2000); HAW. REV. STAT. § 803-45(e), (f) (1987); OKLA. STAT. ANN. tit. 13, § 176.8(E) (West 2008); VA. CODE ANN. § 19.2-67(E) (West 2008); WYO. STAT. ANN. § 7-3-600(r) (2008).

203. *See, e.g.*, United States v. Campagnuolo, 556 F.2d 1209, 1214–15 (5th Cir. 1977) (relaxing the authorization requirement because the offense for which the wiretap was authorized and the offense for which the information was used were so similar that there was no chance that the original wiretap was a "subterfuge" or a pretextual search); United States v. Watchmaker, 761 F.2d 1459, 1470 (11th Cir. 1985) (admitting evidence in a RICO prosecution, even though the Wiretap Authorization specified drug offenses, because the drug offenses were an integral component of the RICO offense). Both cases express the view that the surveillance evidence should be admissible because the connection between the offense specified in the original order and the subsequent plain view offense is close enough that it would be unreasonable to believe that the officers had engaged in a pretextual search.

statutes recognize the importance of erecting procedural barriers to protect against the pretextual seizure of plain view evidence.

Preventing the pretextual use of FISA has become even more critical with the increased importance of electronic communications and the increased invasiveness of surveillance technology. TSP, for example, aims to data mine the electronic communications of all citizens[204] thereby transforming all communications into admissible "plain view" evidence. If FISA evidence is not restricted to foreign intelligence crimes, then there is no reason to believe that evidence gathered under the TSP will be limited to foreign intelligence prosecutions. Moreover, there is little reason to believe that the Executive will be satisfied with the recent expansion of its FISA surveillance power. Echoing the words of his predecessor,[205] Attorney General Alberto Gonzalez called for increased executive discretion: "[t]he operators out at [the National Security Agency] tell me that we don't have the speed and the agility that we need, in all circumstances, to deal with this new kind of enemy . . . . FISA was passed by the Congress in 1978. There have been tremendous advances in technology . . . since then."[206] On July 9, 2008 Congress bowed to this pressure and expanded the FISA surveillance powers to allow the warrantless surveillance of persons "reasonably believed" to be abroad. In passing the FISA Amendment of 2008 Congress increased the chances that FISA will be used pretextually and missed a great opportunity to restore the pre-9/11 balance of security and liberty by limiting the use of FISA's invasive surveillance powers to those foreign intelligence crimes for which it was originally intended.

204. *See* Leslie Cauley, *NSA Has Massive Database of U.S. Calls*, USA TODAY, May 11, 2006, at 1A, *available at* http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm (According to an unnamed source, "[t]he agency's goal is 'to create a database of every call ever made' within the nation's borders"). When the TSP was initially disclosed to the public, reports claimed that the program was limited to international electronic communications but subsequent disclosures indicate that the program's reach may be much greater. *Id.*

205. Just after the 9/11 attacks John Ashcroft made a strikingly similar statement. *See supra* note 172.

206. Press Briefing, The White House, Setting the Record Straight: Democrats Continue to Attack Terrorist Surveillance Program (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2006/01/20060122.html.