University of Miami Law Review

Volume 57 | Number 4 Article 3

7-1-2003

And the Wall Came Tumbling Down: Secret Surveillance After the Terror

William C. Banks

And the Wall Came Tumbling Down: Secret Surveillance After the Terror

WILLIAM C. BANKS*

One inevitable byproduct of the September 11 terrorist attacks has been widespread criticism of what appears to some as a yawning failure of intelligence – why didn't we know enough about the terrorists and their plan to prevent the attack? In the months and years since the calamitous attacks, allegations of failures in gathering, assessing and sharing intelligence information have reached a crescendo. By and large, the critics charge that intelligence agencies failed to "connect the dots," at least in part because the intelligence players – in particular the pertinent divisions within the FBI and CIA – were not talking to one another, or were doing so inefficiently and incompletely. In a December 2002 report, Senate Select Committee on Intelligence vice-chair Richard Shelby described a series of missed signals and misinterpreted leads that, in his mind, could have forewarned of a horrific terrorist attack. Shelby insisted that September 11 "should be an object lesson in the perils of failing to share information promptly and efficiently between (and within) organizations."[1]

Congressional investigators detailed a series of blunders in failing to "connect the dots" before September 11.[2] Failures of information-sharing were supposedly legion: warnings about imminent attacks by Al Qaeda upon U.S. targets were accompanied by intelligence that terrorists might use aircraft as weapons, that operatives would seek training as pilots at U.S. flight schools, and that known Al Qaeda terrorists were residing openly within the United States. The CIA failed to share information about the two known terrorists with the FBI or INS until late August 2001, when efforts to locate them failed. Subsequently, on September 11, the men boarded American Airlines Flight 77 and flew it into the Pentagon. Similarly, when a Phoenix FBI field office agent forwarded his concern about Al Qaeda operatives training at U.S. flight schools, FBI headquarters took no action, at least in part because the

* Laura J. and L. Douglas Meredith Professor, Syracuse University College of Law. The author thanks M. E. (Spike) Bowman, Stephen Dycus, and Peter Raven-Hansen for helpful comments on a draft of this article, and Michael Berner for research assistance.

1. *See* Senator Richard C. Shelby, Vice Chairman, Senate Select Committee on Intelligence, *September 11 and the Imperative of Reform in the U.S. Intelligence Community,* at 5 (Dec. 10, 2002) [hereinafter Shelby Report], *available at* http://intelligence.senate.gov/Shelby.pdf.

2. *See id.* at 3-11.

CIA did not share with the FBI its intelligence indicating that terrorists could use aircraft as weapons.[3] Finally, when Minneapolis FBI field agents grew suspicious of flight school attendee Zacarias Moussaoui in July 2001, their request to headquarters seeking an order permitting secret surveillance of his activities was turned down on the basis that investigators had too little factual information linking Moussaoui to any terrorist organization. Moussaoui is now awaiting trial on charges that he conspired to murder the World Trade Center and Pentagon victims.[4]

The effort to place blame for September 11 has supported the ongoing campaign by the Department of Justice to expand what Attorney General John Ashcroft maintains are essential new tools in the war against terrorism. Some of the new tools that became law in the USA Patriot Act[5] purport to respond directly to alleged shortcomings in the sharing of information between intelligence and law enforcement officials.

Since 1978, the Foreign Intelligence Surveillance Act[6] (FISA) has prescribed procedures for conducting electronic surveillance (and since 1994 for physical searches) within the United States for foreign intelligence purposes. Rules governing law enforcement searches and electronic surveillance are found within the Federal Rules of Criminal Procedure and Title III of the 1968 Crime Control Act, as amended.[7] Although their investigations often overlap, the rules that apply to the two types of investigations are markedly different. Because the Fourth Amendment protects "the people . . . against unreasonable searches and seizures,"[8] the backdrop for both sets of rules is a core protection for individual privacy.[9] When the privacy stakes are higher – when criminal processes and sanctions, including incarceration, may follow – the rules are most protective of the individual and require the government to meet exacting standards before carrying out intrusive investigations. When the aim is to collect foreign intelligence information, the secret and less protective rules and procedures of FISA may be employed. The justifications for using the more permissive FISA mechanism include the fact that the danger of espionage or international terrorism is grave,

---

3. *Id.* at 29.

4. *See* Philip Shenon, *Moussaoui Case May Have to Shift from U.S. Court to Tribunal, Administration Says*, N.Y. TIMES, Feb. 7, 2003, at A13.

5. Pub. L. No. 107-56, 115 Stat. 272 (2001).

6. Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801-1829, 1841-1846, 1861-1863 (West Supp. 2000).

7. Pub. L. No. 90-351, § 802. 82 Stat. 197, 212 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520).

8. U.S. CONST. amend. IV.

9. *See, e.g.*, MARK REIBLING, THE WEDGE: THE SECRET WAR BETWEEN THE FBI AND CIA (1994).

and that the privacy intrusions are limited to the collection of information for foreign intelligence purposes.[10]

The current and at least near-term future climate calls into question the separation of law enforcement and intelligence roles that have been at the center of government's counter terrorism investigative strategy. On the one hand, if the wall between law enforcement and intelligence collection is breached, Congress's objectives in FISA may be thwarted and the Constitution may be violated. On the other hand, if law enforcement and intelligence functions are not permitted to work together effectively to combat terrorism, grave harm to the nation could occur.

In an unprecedented public release of proceedings before the secret FISA tribunal in the summer of 2002, the Foreign Intelligence Surveillance Court (FISC) rejected in part proposed Department of Justice procedures used for coordinating the work of intelligence and law enforcement personnel carrying out surveillance and search activities under FISA, as amended by the Patriot Act. In a unanimous opinion by all seven FISA judges, the FISC ruled that the Criminal Division of the Justice Department could not direct and control surveillance and searches pursuant to FISA for law enforcement ends. The court ruled that having the prosecutors so directly involved in running a FISA investigation would undermine what Congress created – a special mechanism for gathering foreign intelligence information. Further, the judges seemed worried that if the Justice Department proposal were permitted to stand unaltered, important Fourth Amendment interests could be threatened by the substitution of FISA procedures for Title III of the Crime Control Act when the objective of the investigation was to prosecute.

Following this extraordinary decision by the FISC, the government pursued the first-ever appeal under FISA. The inaugural decision of the Foreign Intelligence Surveillance Court of Review (FISCR) in November 2002 reversed the FISC decision and reinstated the Justice Department guidelines that all but eliminate the wall between intelligence collection and law enforcement.[11] As it now stands, the government may take advantage of the secretive and less protective procedures of FISA to plan and carry out surveillance and searches of American citizens, without giving notice or conducting any proceeding before a magistrate. In essence, these activities could be conducted with the primary aim of prosecuting the target.

---

10. The term "foreign intelligence" encompasses counterintelligence and counterterrorism as well as other national security concerns, such as weapons of mass destruction.

11. In re Sealed Case Nos. 02-001, 02-002, 310 F.3d 717 (U.S. Foreign Intell. Surveil. Ct. Rev., 2002) [hereinafter FISCR Opinion].

The FISCR decision is an unfortunate example of overreaching in reaction to the September 11 terror attacks to protect security interests at the expense of individual freedoms and the shared but bounded institutional responsibilities for intelligence gathering and law enforcement. While there are undoubtedly times when avoiding the Title III magistrate and criminal probable cause requirements would facilitate a terrorism investigation, those exceptional instances should occur only when the government meets the requirements of FISA. To the extent that prosecutors might direct and control FISA surveillance for law enforcement purposes following the FISCR decision, the court erred. Whatever else the USA Patriot Act amendments to FISA might have done, they did not eviscerate the distinction between enforcing the laws and gathering intelligence. Neither the Patriot Act nor FISA changed the underlying constitutional protections afforded individuals in the United States.

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.[12] In addition, officials in the Department of Justice contributed to the coordination problem by failing to fully understand how national security investigative authorities differ from those that apply in law enforcement.

This essay will first describe the traditional intelligence and law enforcement roles in counterterrorism. Part II will review the pre-FISA legal context for national security surveillance and searches. Part III includes an assessment of the evolving history concerning the relationship between intelligence and law enforcement in implementing FISA, culminating in the March 2002 procedures that prompted the FISC and FISCR decisions. Part IV will evaluate the FISC and FISCR decisions, identifying statutory and constitutional flaws in both decisions, and looking for common ground between them. Finally, two concluding sections will suggest reforms to FISA and to congressional oversight that can better ensure the shared objectives of security and freedom. These sections also will attempt to clarify where the foreign intelligence/law enforcement overlap stands now.

I. INTELLIGENCE AND LAW ENFORCEMENT IN U.S. NATIONAL SECURITY: ORIGINS OF THE WALL

By now it has become obvious to most observers that our nation's

12. *See, e.g*, RIEBLING, *supra* note 9.

strategies to combat terrorism involve a variety of government functions with overlapping roles and responsibilities, from emergency management and public health, to border and customs protection, to the use of law enforcement and even military force. A major component of our counterterrorism strategy is interdiction – taking efforts to stop the terrorists before they strike. An effective capability to conduct secret intelligence collection is of critical importance in combating terrorism. At the same time, counterterrorism objectives are increasingly being served by criminalizing terrorist acts, as is evidenced by the dozens of new criminal prohibitions on terrorist activities that have been enacted in recent years.

Nonetheless, the divisions in the intelligence community that were formalized with the creation of the Central Intelligence Agency in 1947 were created purposefully. In part, the FBI, and not the CIA, was responsible for domestic security investigations because there was no enthusiasm in the post-World War II years for a secret Gestapo-like agency.[13] The Bureau was always the crime-fighter, but both agencies collected intelligence. It was also the case, however, that intelligence analysts knew the value of having two agencies in partial competition for the same turf. Rivals produce an array of intelligence, and the analyst sifts through it to find what is of worth. Centralizing the intelligence function under one roof might eliminate the advantages of competition.

Fighting crime is like gathering intelligence in that it relies on many of the same techniques to collect information. Information forms the basis of evidence to support convictions and to learn about terrorism or espionage acts before they occur. That information may be found through public sources, through the use of informants, or through searches and electronic surveillance. Law enforcement information must often be shared among the agencies charged with fighting crime and between the grand juries and courts involved in the prosecutions. Of course, unlike traditional law enforcement investigations, intelligence collection operations are secret. Their objective is to learn about the target person or organization, the target's aims and methods, and sometimes to "turn" the target to become an intelligence asset.[14] In addition, the surveillance may continue for months or even years.

In many situations, intelligence officials work alongside law enforcement personnel, and the information gathered in the intelligence

13. *See* JOHN RANELAGH, THE AGENCY: THE RISE AND DECLINE OF THE CIA 104-11 (1986).

14. *See* William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 7 (2000).

operation becomes evidence in an eventual criminal conviction.[15] However, foreign intelligence is also sometimes sought simply to keep tabs on foreign groups, absent any anticipated criminal activity. Foreign intelligence gathering is, therefore, sometimes less targeted and more programmatic than law enforcement collection. Moreover, foreign intelligence information may also be harder for someone outside the intelligence community to evaluate. Pieces may be understood only as part of a mosaic of information, by contrast to the often more specific, historical information obtained for particular law enforcement purposes. Traditional legal standards that insist on particularity, criminality, and eventual notice to the target in law enforcement surveillance and searches are ill-suited for foreign intelligence gathering.

The distinction between these role assignments has never been neat and clean. Instead, intelligence collection and law enforcement roles often overlap, normally in productive ways. Good intelligence work may provide criminal investigators or prosecutors with the tip they need to make a case. Alternatively, the law enforcement team may learn important intelligence information useful for future collection efforts in the course of interrogation or evidence collection in a criminal investigation. In other fundamental ways, however, intelligence and law enforcement investigations are different. Where intelligence collection looks toward preventing future acts, law enforcement usually focuses on a past-completed act. While a criminal investigation normally ends with a decision to prosecute, investigation of the same targets for intelligence purposes may continue even after prosecution.

In recent years, one aspect of the counterterrorism strategy of the United States government has been to increase the collaboration and sharing of information between law enforcement and intelligence investigators. Cooperation and information sharing between intelligence and law enforcement agencies is a formidable task. In part, this challenge is present in any intelligence agency setting because of the tension between the need for security and secrecy and the demand for sharing information. Leaks are anathema, and compromised sources are useless. At the same time, completely secure information is not useful to anyone. As the goals of the different types of investigation are so different, criminal investigators and prosecutors have been counseled repeatedly to stay "clean" – to avoid contaminating possible prosecution evidence through contacts with intelligence officials.[16] Separate cultures have developed within the FBI, for example, where national security and Criminal Divi-

15. *Id.* at 4.

16. *See* Jonathan M. Fredman, *Intelligence Agencies, Law Enforcement, and the Prosecution Team*, 16 YALE L. & POL'Y REV. 331, 337-38 (1998).

sion personnel have traditionally operated in discrete spheres with limited interaction between one another.

Galvanized by the failures in information sharing and cooperation that some maintained might have prevented the September 11 attacks,[17] the Bush Administration, particularly Attorney General Ashcroft, has made a concerted effort to break down these barriers to effective counterterrorism investigations. In essence, the Department of Justice has vigorously promoted a strategy of turning loose all the investigative resources of the nation through the most permissive legal standards available in an effort to prevent terrorist activities in the United States. As the Attorney General noted, the Department of Justice has added a "paradigm of prevention"[18] to that of prosecution in response to terrorist threats. The new paradigm encompasses and increasingly blends the previously discrete intelligence gathering and law enforcement functions. In recent years, and particularly after September 11, criminal investigators and prosecutors are as likely engaged as intelligence officials in the prevention effort. Some would say that FBI counterterrorism agents have long been engaged in prevention, notwithstanding the Attorney General's implication to the contrary.

II. THE PRE-FISA CONTEXT FOR NATIONAL SECURITY INVESTIGATIONS

Throughout much of the 20th century, the executive branch engaged in warrantless electronic surveillance and searches of targets within the United States based on the President's asserted inherent authority to protect the national security.[19] This practice of unmonitored surveillance ebbed during the Vietnam War and civil rights eras as anti-war and civil rights activists were targeted based on a belief that their activities threatened the national security. In many instances the surveillance targeted individuals or domestic groups with no connection to any foreign power.[20] The investigative excesses were curbed in the early 1970s, as government became caught in the fallout from the Watergate

17. *See Joint Inquiry Staff Memorandum: The FBI's Handling of the Phoenix Electronic Communication and Investigation of Zacarias Moussaoui Prior to September 11, 2001*, (Sept. 24, 2002) (statement of Eleanor Hill, Staff Director, Joint Inquiry Staff), *available at* http://www.fas.org/irp/congress/2002_hr/092402hill.html; *see also* REPORT OF THE JOINT INQUIRY INTO THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, S. REP. NO. 107-351, at 1-127 (2002), *available at* http://www.gpoaccess.gov/serialset/creports/911.html.

18. Adam Liptak, *Under Ashcroft, Judicial Power Flows Back to Washington*, N.Y. TIMES, Feb. 16, 2003, at wk5.

19. *See* Foreign Intelligence Surveillance Act of 1978, S. REP. NO. 95-604, at 9-12 (1977).

20. *See* Select Committee to Study Government Operations with Respect to Intelligence Activities, Intelligence Activities and the Rights of Americans, S. REP. NO. 94-755, Book III, at 355 (1976).

scandal, the end of the Vietnam War, and extensive congressional and public disclosures of these prior abuses.

Thirty years ago, before the enactment of FISA, the Supreme Court first confronted the tensions between unmonitored executive surveillance and individual freedoms in the national security setting. *United States v. United States District Court*[21] arose from a criminal proceeding in which the United States charged three defendants with conspiracy to destroy government property – a planned dynamite bombing of a CIA office in Ann Arbor, Michigan.[22] During pretrial proceedings, the defendants moved to compel disclosure of electronic surveillance. In response, although the Government admitted that a warrantless wiretap had intercepted conversations involving the defendants, it defended its actions in the Supreme Court on the basis of both the Constitution and a national security disclaimer in the 1968 Crime Control Act.[23]

Justice Powell's opinion for the Court rejected the statutory argument and concluded that the Crime Control Act disclaimer of any intention to legislate regarding national security surveillance had not created executive powers, but had simply left presidential powers in the area untouched.[24] Turning to the constitutional claim, the Court found authority for national security surveillance implicit in the President's Article II Oath Clause, which includes the power "to protect our Government against those who would subvert or overthrow it by unlawful means."[25] However, the "broader spirit" of the Fourth Amendment, and "the convergence of First and Fourth Amendment values" in national security wiretapping cases, made the Court especially wary of possible abuses of the national security power.[26] Justice Powell then proceeded to balance "the duty of Government to protect the domestic security, against the potential danger posed by unreasonable surveillance to individual privacy and free expression."[27] In rejecting the Government's position, he concluded that waiving the Fourth Amendment probable cause requirement and allowing "unreviewed executive discretion" could lead the executive to "yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and

21. 407 U.S. 297 (1972) [hereinafter Keith] (The decision is usually referred to by the name of the district court judge who first heard it, Damon J. Keith).

22. *Id.*

23. *Id.* at 302-03 (The Omnibus Crime Control and Safe Streets Act emphasized the President's inherent constitutional power to protect national security free of any limitations); *see* Pub. L. No. 90-351, § 802, 82 Stat. 197, 212 (1968).

24. *Keith*, 407 U.S. at 306.

25. *Id.* at 310; *see also* U.S. CONST. art. II., § I.

26. *Keith*, 407 U.S. at 313.

27. *Id.* at 314-15.

protected speech."[28]

The government argued for an exception to the warrant requirement, citing both the unique characteristics of ongoing national security surveillance and fear that leaks could endanger sources and methods of intelligence gathering. Justice Powell, however, answered that the potential for abuse of the surveillance power in this setting, along with the capacity of the judiciary to manage sensitive information in *ex parte* proceedings, rendered any inconvenience to the government "justified in a free society to protect constitutional values."[29]

Justice Powell was careful to emphasize that the case involved only domestic targets of surveillance, and that the Court was not expressing an opinion on the discretion to conduct surveillance when foreign powers or their agents are targeted. Finally, the Court left open the possibility that different warrant standards and procedures than those required in normal criminal investigations might be applicable in a national security investigation, presumably even one not involving foreign intelligence.

> We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.' The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.[30]

The Court implicitly invited Congress to promulgate a set of standards for these types of surveillance:

> Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to *the legitimate need of Government* for *intelligence information* and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of the citizen rights deserving protection.[31]

Although Congress did not react immediately to the *Keith* decision, Justice Powell's opinion provided an important impetus for the development of what would become FISA. Like the Supreme Court, Congress

28. *Id.* at 317.
29. *Id.* at 319-21.
30. *Id.* at 323.
31. *Id.* at 322-23 (emphasis added).

recognized that warrantless surveillance by the executive branch could undermine important constitutional values at the confluence of the First and Fourth Amendments. At the same time, Congress came to appreciate that the nature and purpose of intelligence investigations differ considerably from those of criminal law enforcement investigations. Congress recognized that the traditional warrant requirement practiced by law enforcement might not be the best model for assuring a fair balance between security and liberty in national security investigations seeking foreign intelligence.[32]

While the *Keith* decision served as the constitutional foundation for FISA, another surveillance dispute was ongoing when FISA was enacted. In 1976, a Vietnamese citizen living in the United States began sending packages to Vietnamese government officials in Paris, through a Vietnamese-American who also happened to be a CIA agent.[33] The Department of Justice undertook a warrantless search of one of the packages. Although the courier was authorized to open and inspect the package, that permission was not given on the basis of any asserted foreign intelligence exception to the warrant requirement, but rather on the grounds that there was no reasonable expectation of privacy regarding the contents of the package. After this inspection revealed that classified documents were being delivered to a Vietnamese official in Paris, the Attorney General obtained the President's personal approval to search subsequent packages that would normally have been protected by a reasonable expectation of privacy. The Attorney General also approved a wiretap of the target's telephone.[34] Once intelligence officials learned that the source of the classified documents was a U.S. citizen employed by the United States Information Agency, the Attorney General authorized covert television surveillance of the citizen's office.[35]

The criminal division of the Justice Department was informed of the status of the investigation on a regular basis, and the USIA employee and the Vietnamese-American were indicted, in January 1978. After the defendants challenged the constitutionality of the package searches and electronic surveillance, the district court held an evidentiary hearing and ruled that on July 20, 1977, the investigation had become "primarily a criminal investigation."[36] Thus, the searches and surveillance conducted

32. United States v. Humphrey, 456 F. Supp. 51, 58-59 (E.D. Va. 1978). Congress has never created procedures for surveillance or searches in national security investigations where no foreign intelligence or connection to a foreign power is suspected. By default, then, such investigations are subject to Title III and Rule 41.

33. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 911 (4th Cir. 1980).

34. *Id.* at 912.

35. *Id.*

36. *Id.* at 916.

before July 20 were viewed as being primarily in pursuit of foreign intelligence information. Focusing on the purposes of the surveillance, rather than the investigation's purpose, the district court ruled that the warrantless searches and surveillance before July 20 were lawful, consistent with *Keith*, because their primary purpose was the pursuit of foreign intelligence information.[37] However, evidence derived from the same searches and surveillance after July 19 was suppressed. On appeal, the government argued that "if surveillance is to any degree directed at gathering foreign intelligence," the traditional warrant requirement should not apply.[38] In response, the defendants argued that any exception to the warrant requirement could not apply unless the search or surveillance was conducted "solely" to gather foreign intelligence.[39] The Fourth Circuit Court of Appeals rejected these polar alternatives in favor of a middle ground, holding that the executive branch "should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons."[40]

As developed by the *Truong* court, the "primary purpose" doctrine reflects the court's view of what the Fourth Amendment requires. Any lesser standard would presumably be unconstitutional. At the same time, "primary purpose" is treated as a qualitative standard that invites after-the-fact subjective judgments during evidentiary hearings, where judges are inclined to defer to the decisions of intelligence professionals. Additionally, in the midst of an investigation, the need for speedy action, along with problems of coordination among law enforcement and intelligence agencies, means that the intelligence professionals make these "primary purpose" decisions, not a magistrate. The theory, however, is that once an investigation becomes primarily criminal in nature, the courts are entirely competent to make the usual probable cause determination when surveillance or search authority is sought, and individual privacy interests come to the fore when the government attempts to lay the foundation for a criminal prosecution.

Congress enacted FISA while the *Truong* appeal was pending and practically mooted the issue of whether warrantless electronic surveillance within the United States for foreign intelligence purposes is constitutional.[41] FISA implemented exclusive standards for conducting

37. *Id.* at 915.

38. *Id.*

39. *Id.*

40. *Id.*

41. I say "practically" because, in theory, Congress cannot legislate to deny surveillance authority that is part of a core Article II power of the executive. While the executive branch has worked within FISA for 25 years, it remains possible that new threats or conditions could give rise to renewed claims for warrantless executive branch surveillance authority.

electronic surveillance for foreign intelligence purposes within the United States,[42] and added similar standards for physical searches in 1994.[43] The procedures and criteria for deciding what circumstances would permit the issuance of surveillance and search orders emerged through twenty-four years of practice under FISA. The federal courts have repeatedly construed these procedures and criteria to be adequate substitutes for the traditional law enforcement warrant, satisfying the Fourth Amendment's "reasonableness" requirement.[44] Central to the development of this body of case law upholding the FISA procedures has been the principle that FISA was designed for the gathering of foreign intelligence information and that any criminal prosecution that follows from surveillance undertaken pursuant to FISA has been incidental to the purpose of gathering foreign intelligence information.

FISA authorizes the Attorney General to approve applications for orders to conduct electronic surveillance or physical searches within the United States for the purposes of foreign intelligence if there is probable cause to believe that the target is a "foreign power"[45] or "agent of a foreign power."[46] The Act also requires that "an executive branch official . . . employed in the area of national security or defense [certify to the FISC] that a significant purpose of the [FISA surveillance or search] is to obtain foreign intelligence information."[47] In addition, FISA seeks to ensure that intelligence officials are conducting their searches and surveillances strictly for foreign intelligence purposes by requiring that each certification designate the type of foreign intelligence information being sought and explain the basis for this designation. FISA also provides for limited judicial review of those certifications.

Before the FISC issues an order approving electronic search or surveillance involving a U.S. person,[48] the FISC judge must find probable cause that the target is an agent of a foreign power, based on meeting

42. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 1801(f)(1)-(4),92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1829, 1841-1846, 1861-1863 (1978)).

43. Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 302(a)(1), 108 Stat. 3423 (1994).

44. *See, e.g.*, United States v. Duggan, 743 F.2d 59 (2d Cir. 1984); United States v. Johnson, 952 F.2d 565, 575 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); United States v. Ott, 827 F.2d 473, 475-77 (9th Cir. 1987).

45. 50 U.S.C. § 1801(a) (1994).

46. 50 U.S.C. § 1801(b) (2003) (amended by Act of Dec. 3, 1999, Pub. L. No. 106-120, 113 Stat. 1606, 1619-20).

47. 50 U.S.C. §1823(a)(7) (2001); *see* 50 U.S.C. §§ 1804(a)(7)(A),(B) (2001), and §§ 1823(a)(7)(A), (B) (2001) (concerning electronic surveillance and search provisions).

48. The Act defines "United States person" to include a citizen of the United States, an alien lawfully admitted for permanent residence, and an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence. 50 U.S.C. § 1801(i) (2001).

one of four conditions: (1) the target knowingly engages in clandestine intelligence activities on behalf of a foreign power, which "may involve" a criminal law violation; (2) the target knowingly engages in other secret intelligence activities on behalf of a foreign power pursuant to the direction of an intelligence network, and those activities involve or are about to involve criminal law violations; (3) the target knowingly engages in sabotage or international terrorism or is preparing for such activities;[49] or (4) the target knowingly aids or abets another who acts in one of the above ways.[50] The connection to national security crimes is thus explicit, but the predicate for obtaining permission to conduct secret surveillance or search is by showing probable cause that the target is a foreign agent, not probable cause that the target is involved in a crime.

Many criminal defendants since 1978 have asserted that certain FISC-approved surveillance was not in fact conducted for the primary purpose of foreign intelligence collection.[51] In each such challenge, the federal courts sustained the FISA surveillance under the *Truong* "primary purpose" test. While FISA demands that "the purpose" of any surveillance or search be the gathering of foreign intelligence, a FISC judge in each case granted approval of the surveillance or search and found its primary purpose to be the pursuit of foreign intelligence or foreign counterintelligence information. These initial rulings strengthened the government's defenses in federal courts.

III. FISA AND THE INTELLIGENCE/LAW ENFORCEMENT OVERLAP

The path from the Supreme Court's *Keith* decision to FISA lays bare the kind of exceptional authority Congress was willing to provide in the name of protecting national security. Early on, one Senate bill would have made intelligence surveillance authority part of Title 18, the title reserved for crimes and criminal procedure. Even so, the drafters stated that authorized surveillance would be for foreign intelligence purposes.[52] Eventually this proposal was removed from Title 18 and placed in Title 50, War and National Defense, a better fit since the bill estab-

49. FISA defines "international terrorism" to include activities that (1) involve violent acts dangerous to human life that . . . would be a criminal violation if committed within the jurisdiction of the United States or any State; (2) appear to be intended (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping; and (3) occur totally outside the United States, or transcend national boundaries. *See* 50 U.S.C. § 1801(c) (2003).

50. 50 U.S.C. § 1801(b)(2) (1994).

51. *See, e.g.*, United States v. Truong Dinh Hung, 629 F. 2d 908, 913 (4th Cir. 1980); United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982); United States v. Megahey, 553 F. Supp. 1180 (E.D.N.Y. 1982).

52. *See* H.R. REP. No. 95-1283 (1978) ("[i]f enacted, this legislation would require a judicial warrant authorizing the following for foreign intelligence purposes.").

lished procedures dealing with the collection of foreign intelligence.[53] Congress also recognized from the beginning that "no United States citizen in the United States should be targeted for electronic surveillance by his government absent some showing that he at least may violate the laws of our society,"[54] but also recognized that evidence of such national security crimes may be gathered during surveillance. This association with criminality was undoubtedly designed to forestall a return to the days of politically motivated surveillance of U.S. citizens, but it also shows that, while a suspicion of criminal activity is considered essential when targeting U.S. citizens, Congress did not intend for FISA to in any way authorize surveillance for law enforcement purposes. At the same time, the drafters of FISA understood that intelligence gathering and law enforcement would overlap in practice. Periodic oversight reviews of FISA underscore congressional understanding that FISA-derived information would sometimes be used in prosecutions.[55]

In the years since 1978, the emerging confluence of intelligence gathering and law enforcement as elements of counterterrorism strategy has strained the capacities of both FISA procedures and FBI personnel attempts to manage the relationship between intelligence and law enforcement. On the one hand, as the Department of Justice maintained, "there is no dichotomy between intelligence and law enforcement efforts to protect against terrorism and espionage."[56] The enactment of dozens of criminal prohibitions on terrorist activities and espionage has added to the contexts in which surveillance may simultaneously be contemplated for intelligence gathering and law enforcement purposes. On the other hand, despite the blurring of previously sharper lines between intelligence collection and law enforcement, FISA's special set of procedures remains the seminal authority when the government's purpose is that of gathering foreign intelligence. As the Senate Intelligence Committee report opined in 1984, "the 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 surveil-

53. *See* H.R. REP. No. 95-7308 (1978) ("[b]ecause the bill instead establishes authorities and procedures dealing with the collection of foreign intelligence, the committee believes that its proper placement would be in title 50").

54. *See id.* (emphasizing that a U.S. citizen "should be able to know that his government cannot invade his privacy with the most intrusive techniques if he conducts himself lawfully.").

55. The Foreign Intelligence Surveillance Act of 1978: The First Five Years, S. REP. No. 98-660 at 14 (1984) [hereinafter First Five Years] ("FISA surveillance would be . . . part of an investigative process often designed to protect against the commission of serious crimes such as . . . terrorist acts. . . . Intelligence and law enforcement tend to merge in this area.").

56. Supplemental Brief of the Department of Justice for the United States at 8, In re Sealed Case, 310 F.3d 717 (Foreign Intelligence Surveillance Ct. Rev. 2002) (No. 02-001).

lance will also produce some foreign intelligence information."[57] And although the Patriot Act changed the weighing of the relative importance of foreign intelligence and prosecution objectives in surveillance, the core focus on intelligence remains.

Whatever the functional overlap, the procedural differences between surveillance and searches for law enforcement and for gathering foreign intelligence are stark. FISA permits electronic surveillance or search if the FISC finds that there is probable cause to believe that the target of the surveillance is a foreign power or agent of a foreign power.[58] Conversely, Title III permits electronic surveillance only where there is probable cause to believe that "an individual is committing, has committed, or is about to commit"[59] a serious crime, and "particular communications concerning that offense will be obtained through such interception."[60] While FISA surveillance may be authorized for ninety days,[61] Title III collection is limited to thirty days until renewal before a judge is required.[62]

Normally, the target of FISA surveillance or a physical search is not entitled to notice that the FISA-authorized activities occurred unless the information obtained is used in a subsequent criminal prosecution.[63] By contrast, criminal searches pursuant to the Federal Rules of Criminal Procedure usually require immediate notice,[64] and Title III surveillance targets must be given notice within ninety days of termination.[65] Moreover, a criminal defendant that has been subject to FISA surveillance or search is normally not entitled to review the background materials that supported the FISC order – the application, affidavits, surveillance logs, or statements from informants that supported the FISC order.[66] No court has in fact ordered disclosure. In law enforcement, however, criminal defendants routinely obtain access to these types of documents.[67] These differences are attributable to the fact that Congress recognized that collection of foreign intelligence requires secrecy, and believed that the dis-

57. First Five Years, *supra* note 55, at 15.

58. 50 U.S.C. § 1805(a)(3) (2000).

59. 18 U.S.C. § 2516 (2000).

60. *Id.* §§ 2518(3)(a)-(b) (2000).

61. 50 U.S.C. § 1805(d)(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 an agent of a foreign power). *See also* 50 U.S.C. § 1805(e)(1) (2000).

62. 18 U.S.C. § 2518(5) (2000).

63. 50 U.S.C. §§1806(c), 1825(d) (2000).

64. FED. R. CRIM. P. 41(d).

65. 18 U.S.C. § 2518(8)(d) (2000).

66. 50 U.S.C. §§ 1806(f), 1825(g) (2000). (A reviewing court reviews these materials *ex parte* and *in camera* and only discloses them to the defendant "where disclosure is necessary to make an accurate determination of the legality of the surveillance/search.").

67. *See, e.g.*, 18 U.S.C. § 2518(9) (2000).

tinct purposes of foreign intelligence surveillance merited a departure from the strict criminal law standards, even for especially intrusive surveillance.[68]

In July 1995, the Attorney General issued a directive concerning the FISA law enforcement/intelligence overlap.[69] The 1995 Procedures were adopted because back-channel coordination between intelligence and law enforcement officials had grown, particularly during the Aldrich Ames espionage investigation in 1993. This coordination reached the point where the Justice Department's Office of Intelligence Policy and Review (OIPR) – a gatekeeper between the criminal and intelligence sides in FISA applications – advised the Attorney General that Ames' lawyers could use an alleged close intelligence/law enforcement relationship in Ames' case to cast doubt on the primary purpose of the FISA surveillance and possibly derail the prosecution.[70] Although Ames' plea bargain resolved the immediate problem, the 1995 Procedures limited the nature and extent of law enforcement/intelligence consultations thereafter. Advice could still be given, but the advice should "not inadvertently result in either the fact or the appearance of the Criminal Division's *directing or controlling*" an investigation.[71]

Apparently, however, the 1995 guidelines were misunderstood within the Department. OIPR lawyers interpreted FISA as practically forbidding contact between intelligence officials and criminal investigators. As the General Accounting Office later reported, intelligence coordination with law enforcement dropped off after issuance of the 1995 guidelines, and the contact that did occur came so late in the process as to be practically useless.[72] According to another Justice Department report, the restrictions imposed in practice by OIPR prevented the FBI from obtaining "meaningful advice from the Criminal Division during an FCI [foreign counterintelligence] investigation."[73] During this period, the FBI developed a parallel system of "dirty" teams for intelligence gathering and "clean" teams for law enforcement. They could

68. *See, e.g.*, S. REP. NO. 95-701, at 12-15 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3980-81, 3983.

69. Memorandum from the Attorney General, Procedures for Contacts Between the FBI and Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations (July 19, 1995) [hereinafter 1995 Procedures].

70. STEPHEN DYCUS, ARTHUR BERNEY, WILLIAM C. BANKS & PETER RAVEN-HANSEN, NATIONAL SECURITY LAW 679-80 (3d ed. 2002).

71. *Id.* at ¶ A6 (emphasis added).

72. *See* Shelby Report, *supra* note 1, at 49 (citing GENERAL ACCOUNTING OFFICE, COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED (2001)).

73. *Id.* (citing Department of Justice, *Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation*, (May 2000), *available at* http://www.usdoj.gov/ag/readingroom/bellows/htm.

work at the same time on the same targets, yet they rarely talked to one another.[74] The "walls" were effectively erected by OIPR whenever an intelligence investigation revealed some indication of criminal activity.

Between 1995 and 2002, the FISA procedures were augmented on a few occasions to permit more information sharing between those seeking foreign intelligence and the Criminal Division. Among other things, the procedures permitted the reporting of reasonable indications of significant federal crimes to the Criminal Division, consulting between the Criminal Division and national security personnel, and providing guidance to the FBI "aimed at preserving the option of criminal prosecution," although the Criminal Division was not allowed "to direct or control the FISA investigation."[75] Throughout this period, the FISC relied on and approved the new FISA procedures. Where there were separate intelligence and law enforcement investigations of the same target or targets, or a single investigation with overlapping intelligence and law enforcement interests, the FISC approved case-specific information screening "walls" proposed by the government in its FISA applications. The wall mechanisms ranged from the simple – preventing criminal investigators or prosecutors from having access to raw FISA materials, and having a neutral screener review the raw material and pass along only the materials that might become pertinent evidence in a prosecution – to the complex – where the FISC itself served as the wall, such as during investigations involving the bombing of the Africa embassies in 1998 where criminal and intelligence investigations were going on in the United States and abroad concurrently and prosecution was a likely objective from the start.[76]

As espionage and terrorism incidents and threats against U.S. interests escalated, pressure on the wall began to build. In 1999, the high-profile and ultimately embarrassing Wen Ho Lee espionage investigation prompted the Attorney General to commission a review team to assess the Lee investigation and to make recommendations concerning, among other things, FISA.[77] Headed by Assistant U.S. Attorney Randy Bellows, the team concluded that the FBI should have sought and obtained FISA surveillance of Dr. Lee, and that OIPR conservatism in reviewing FISA applications caused the Department to insist on more

74. *Id.* at 50 (citing Roberto Suro, *FBI's 'Clean' Team Follows 'Dirty' Work of Intelligence*, WASH. POST, Aug. 16, 1999, at A13).

75. In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 619 (U.S. Foreign Intell. Surveil. Ct. 2002) [hereinafter FISC Decision].

76. *Id.* at 620.

77. *See* Department of Justice, *Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation* (May 2000) [hereinafter Bellows Report], *available at* http://www.usdoj.gov/ag/readingroom/bellows/htm.

probable cause than the law requires.[78]

Then came September 11. The post-September 11 finger pointing included allegations that the wall had stood in the way of sharing information that might have slowed or thwarted the terrorist attacks. Most prominent are recurring allegations that FBI adherence to the wall prevented authorities from learning enough about alleged hijacker Zacarias Moussaoui in the summer of 2001 to have prevented the September 11 attacks. Moussaoui arrived in the United States on a French passport and first enrolled in flight training in Oklahoma.[79] After some weeks, he dropped out of the Oklahoma program and moved to Minnesota, where he sought flight training at a school that had a simulator for large passenger airliners.[80] FBI field agents reportedly learned that he paid for flight training in cash, that he was not a good pupil, and that he showed interest in learning how to fly commercial airliners. Although he was by then subject to unobtrusive physical observation, no search of his home, computer, or other possessions took place, nor was any electronic surveillance conducted. Minneapolis field office FBI agents wanted to examine his computer and personal papers after he was taken into government custody for overstaying his tourist visa, but the law enforcement investigators had no probable cause to believe that he was engaged in, or was about to engage in, criminal activity. FBI Headquarters initially considered seeking a warrant for a law enforcement search. Simultaneously, however, 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.

The Minneapolis agents decided against seeking a traditional law enforcement warrant, apparently because of doubts about being able to meet the probable cause standard. Instead, they sought permission to request a FISA order on the assumption that the probable cause showing is easier to demonstrate before the FISC.[81] However, when FBI field agents sought permission to use the FISA procedures to enable secret gathering of intelligence information, they were again denied by Headquarters on the grounds that the Bureau lacked sufficient information connecting Moussaoui to any foreign power.[82] Although field agents submitted a lengthy written request to Headquarters, the agents at Head-

78. *See id.* at 492 (*cited in* STAFF OF SENATE JUDICIARY COMMITTEE, FBI OVERSIGHT: FISA IMPLEMENTATION FAILURES at 23-24 (Feb. 2003), (interim report submitted by Senators Leahy, Grassley, and Spector) [hereinafter Interim Report].

79. *See Joint Inquiry Staff Memorandum*, *supra* note 17, at 14.

80. *Id.* at 15.

81. *Id.* at 16.

82. *Id.* at 17.

quarters only orally briefed the lawyers responsible for making the foreign agency recommendation. In addition, the Headquarters agents did not conduct any computer searches for information that may have been relevant to the Moussaoui request. If they had, then agents could have had access to a July 2001 memorandum from the FBI special agent in Phoenix regarding both the Usama bin Laden Unit and the Radical Fundamentalist Unit within the FBI counterterrorist infrastructure. The memorandum warned about potential dangers from Al Qaeda affiliates training at U.S. flight schools. Agency personnel apparently decided not to follow up on the memorandum, and no managers or senior officials saw the memorandum before September 11.[83]

If the document had been shared and considered, it would certainly have added context to Moussaoui's conduct, and been relevant toward a finding of probable cause.[84] To make matters worse, the FBI attorneys apparently misled the Minneapolis agents in advising that FISA required evidence that Moussaoui had connections to a recognized terrorist organization, one on the list of State Department terrorist organizations.[85] After three weeks of searching, French intelligence officials reported to the FBI only an unconfirmed account that Moussaoui once traveled with a French Muslim acquaintance to fight in the new jihad against Russia in Chechnya.[86] On September 11, after the attacks, the Minneapolis agents were able to obtain a criminal search warrant to search Moussaoui's computer and personal effects. Except for taking note of the attacks, an admittedly significant development, the application contained the same information that had been previously determined to be insufficient to meet FISA requirements.[87]

Although the FBI has been subject to much scapegoating for the perceived missed opportunity with Moussaoui, the responsible legal advisers at the Bureau were simply paying close attention to their legal authority. It was the agents and junior lawyers at FBI Headquarters who apparently insisted, with no legal basis, that foreign agency be found on the basis of connections to a recognized terrorist group, much less an organization designated as such by the Secretary of State.[88] What did have legal support, however, was the senior agents' understanding that "agent of a foreign power" is a fact-based inquiry, tied to terrorist activity; the one unconfirmed report in FBI possession that Moussaoui had

83. Shelby Report, *supra* note 1, at 29-30.

84. Interim Report, *supra* note 78, at 15-16, 26.

85. Shelby Report, *supra* note 1, at 53; *see also id*, at 20.

86. Seymour M. Hersh, *The Twentieth Man*, THE NEW YORKER, Sept. 30, 2002, at 56.

87. Interim Report, *supra* note 78, at 17.

88. Shelby Report, *supra* note 1, at 53.

urged another French Muslim to fight in Chechnya counted as an attenuated stretch, at best, toward a finding of foreign agency.

Still, when Attorney General Ashcroft sought additional authority to investigate terrorist threats in the weeks after September 11, Congress was compliant. Former general counsel of the National Security Agency Stewart Baker complained that "barriers to information-sharing between intelligence and law enforcement agencies have already cost us dearly in the fight against terror."[89] Officials reasonably maintained that counterterrorism investigations are now, more than ever, simultaneously expected to be concerned with prevention of terrorist activities and apprehension of criminal terrorists.

In the rush to "do something" in response to September 11 and to accommodate the demands of the administration for greater authority, Congress passed the 352-page USA Patriot Act[90] after only a few weeks of hearings and limited debate. The Act amended FISA in a few particular respects, and two sections effectively lowered the barrier between law enforcement and intelligence gathering in seeking FISA orders. Instead of foreign intelligence collection being "the purpose" (interpreted as "primary purpose") of the surveillance, it now must be only a "significant purpose" of the search or wiretap.[91] Congress also added an information-sharing provision to FISA. The new section permits the officials who conduct electronic surveillance to acquire foreign intelligence to "consult with Federal law enforcement officers to coordinate efforts to investigate or protect against" terrorist activities by foreign powers or their agents.[92] The same section states that such coordination "shall not preclude" the government's certification that a "significant purpose" of the surveillance requested is to obtain foreign intelligence information.[93]

The imperative to act swiftly after September 11 meant that no one, and certainly not Congress, gave careful consideration to a comprehensive review of FISA or intelligence authorities generally. FISA was largely untouched by the Patriot Act, and its essence remains foreign intelligence collection. Perhaps cognizant that the intelligence gathering/law enforcement roles would be further blended and merged in light of the Patriot Act changes, the FISC responded to the first set of FISA applications filed under the revised Act, in November 2001, by formaliz-

89. Stewart Baker, *Grand Jury Secrecy Rules Help the Terrorists*, WALL ST. J., Oct. 5, 2001, at A14.

90. Pub. L. No. 107-56, 115 Stat. 272 (2001).

91. *Id.* at § 218, 115 Stat. 272, 291 (amending 50 U.S.C. §§ 1804(a)(7)(B), 1823 (a)(7)(B)).

92. *Id.*, at § 504(a), 115 Stat. 272, 364-365 (amending 50 U.S.C. § 1806(k)(1)).

93. 50 U.S.C. § 1806(k)(2) (2000) (*amended by* USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 364-65 (2001)).

ing the augmented 1995 Department of Justice Procedures as "minimization procedures" to apply to all future applications to the FISC.

To reduce the risk that FISA surveillance could interfere with privacy rights, the Act has since 1978 required that procedures be adopted by the Attorney General and followed to the satisfaction of the FISC to "minimize the acquisition and retention, and prohibit the dissemination" of nonpublic information about U.S. persons.[94] Although the procedures are classified, they include some standard review mechanisms and some situation-specific assessments.[95] FISA prohibits disclosure of FISA-derived information except as provided by the minimization procedures,[96] although another section authorizes dissemination of FISA material for law enforcement purposes that is also evidence of a crime.[97] The effect of the November 2001 FISC order was to transform the Justice Department procedures that had been subject to case-by-case adjustments into binding procedures that govern every FISA application.

Despite the FISC order, the Department of Justice issued March 2002 Intelligence Sharing Procedures designed to supersede prior procedures to take into account the "significant" purpose and information sharing amendments to FISA. The Procedures parrot the Patriot Act and claim that the Act "allows FISA to be used primarily for a law enforcement purpose, as long as a significant foreign intelligence purpose remains."[98] The March 2002 Procedures also permit an exchange of a "full range of information and advice" between intelligence and law enforcement officials regarding "the initiation, operation, continuation, or expansion of FISA searches or surveillance," and providing that such coordination "shall not" preclude the certification to the FISC of a significant foreign intelligence purpose.[99]

IV. THE MAY 2002 FISC OPINION

Following approval by the Attorney General of the March 2002 procedures, the Department of Justice certified an application for surveillance to the FISC and, as part of the application, also moved that the FISC vacate its minimization and "wall" procedures to the extent they are inconsistent with the new Department procedures. For the most part,

94. 50 U.S.C. §§ 1801(h), 1805(a)(4) (2000).

95. William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 89 (2000).

96. 50 U.S.C. § 1806(a) (2000).

97. 50 U.S.C. § 1801(h)(3) (2000).

98. Memorandum from the Attorney General, Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI 2 (Mar. 6, 2002).

99. *Id.*

the FISC judges agreed. Although the public did not know about the court's decision until a nearly unprecedented[100] public statement in August 2002, all ten judges then on the FISC,[101] along with the past presiding judge of the FISC, agreed to publish an opinion of May 17, signed by all seven judges of the FISC.[102]

Accepting the Department of Justice invitation, the FISC ordered that the March 2002 procedures be adopted as minimization procedures to apply in all cases. However, the court also ordered modifications to those procedures, based on its interpretation of FISA. The FISC styled its partial repudiation of the DOJ procedures as a straightforward application of the requirements for minimization of the acquisition, retention, and dissemination of information obtained through electronic surveillances and physical searches of U.S. persons. In the opinion of the FISC, the proposed Justice Department procedures would not adequately minimize the uses of information obtained through FISA processes. Because the court determined that the Department's procedures did not comply with the necessary minimization requirements, the FISC did not respond directly to the Department arguments that the Patriot Act amendments to FISA authorized the changed procedures in their entirety.

As the FISC perceived the Justice Department's proposed procedures, the FISC would now be balancing the use of FISA materials "against the government's need to obtain and use evidence for criminal prosecution,"[103] instead of using minimization principles to determine the "need of the United States to obtain, produce, and disseminate foreign intelligence information."[104] According to the FISC, portions of the Department's procedures would permit the existing useful coordination among intelligence and law enforcement agencies to become subordination of the former to the latter. Although the Patriot Act authorizes consultation between intelligence and law enforcement officers to "coordinate efforts to investigate or protect against" foreign threats to national

100. In 1981, in FISC's only previous public statement, Presiding Judge Hart issued a brief opinion for the FISC affirming that the court had no jurisdiction to issue warrants for physical searches. *See In the Matter of the Application of the United States for an Order Authorizing the Physical Search of Nonresidential Premises and Personal Property* (1981).

101. That ten judges approved publication of an opinion signed by seven judges reflected an increase in the number of judges sanctioned by the Patriot Act. *See* USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 283 § 208 (2001) (amending 50 U.S.C. 1803(a)).

102. FISC Decision, 218 F. Supp. 2d 611 (2002). The May 17 Order was subsequently incorporated and implemented in a July 19, 2002, decision denying a FISA application in Case Number 02-662. *See* United States Foreign Intelligence Surveillance Ct. of Rev., Hearing Transcript 5 (Sept. 9, 2002) (No. 02-001) [hereinafter Hearing Transcript].

103. *FISC Decision*, 218 F. Supp. 2d at 624.

104. *See* 50 U.S.C. §§ 1801(h), 1821(4) (2003).

security,[105] the limits drawn by the FISC on Department of Justice procedures seek to avoid FISA activities where "criminal prosecutors direct both the intelligence and criminal investigations . . . [and] coordination becomes subordination of both investigations or interests to law enforcement objectives."[106] The court explained what it viewed as the dangerous implications of the DOJ procedures:

> [C]riminal prosecutors will tell the FBI when to use FISA (perhaps because 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 and when use of FISA can cease because there is enough evidence to arrest and prosecute.[107]

The FISC judges worried that under the DOJ's procedures, prosecutors would have "every legal advantage conceived by Congress to be used by U.S. intelligence agencies to collect foreign intelligence information," including the lesser probable cause standard, use of "the most highly advanced and intrusive techniques for intelligence gathering," and discretion to carry on surveillances and searches for a long time.[108] All of these powers could be employed after finding only "that the U.S. person is . . . using or about to use the places to be surveilled and searched, without any notice to the target unless arrested and prosecuted, and, if prosecuted, no adversarial discovery of the FISA applications and warrants."[109] After concluding that it was not persuaded that criminal prosecutors needed such intrusive means to obtain foreign intelligence information, the *en banc* FISC struck two paragraphs of the DOJ procedures (those permitting prosecutors to advise FBI intelligence officials concerning "the initiation, operation, continuation, or expansion of FISA searches or surveillance") and replaced them with the "bright line" language similar to the 1995 admonition that law enforcement personnel should not "direct or control" the use of FISA procedures, along with a requirement that consultations and coordination be monitored by OIPR.[110]

The essence of the FISC decision was to order preservation of the foreign intelligence objective of FISA. Thus, the FISC order that the Criminal Division not make recommendations concerning "the initiation, operation, continuation or expansion" of FISA surveillance or searches, that prosecutors not "direct or control . . . to enhance criminal

105. 50 U.S.C. §§ 1806(k), 1825(k) (2000).

106. *FISC Decision*, 218 F. Supp. 2d at 623-24.

107. *Id.*

108. *Id.*

109. *Id.*

110. *Id. at* 611.

prosecution,"[111] and that it not recommend that an existing FISA search or surveillance be conducted in a particular way or be in pursuit of particular information was an attempt by the court to preserve the distinction between law enforcement and foreign intelligence objectives in carrying out FISA activities that Congress enshrined in FISA in 1978. Likewise, what became known as the "chaperone" requirement, that the OIPR had to "be invited" to participate whenever law enforcement and intelligence officials consult on a FISA matter,[112] reflected a well-intended if cumbersome desire to monitor what remained of the protective wall between law enforcement and intelligence gathering. If OIPR representatives were unable to attend the meetings, the procedures as approved by the FISC required that OIPR be "apprized of the substance of the meetings forthwith in writing so that the [FISC] may be notified at the earliest opportunity."[113]

The FISC choice to base its decision on the minimization requirements in FISA became an easy target for the government and the FISCR on appeal of the FISC decision. Although the 2002 Justice Department procedures, as amended by the FISC, are designed to meet the demands for minimization under FISA, the FISC decision likely would have been more difficult to overturn had the judges responded directly to the Patriot Act claims made by the DOJ. To be sure, all seven judges left little doubt that they would have culled out the same few offensive portions of the DOJ procedures in directly responding to the Patriot Act amendments.[114] Still, those less-versed in FISA than the seven judges (that means almost everyone else, including the FISCR and the media)[115] had a difficult time understanding how an express authorization for information sharing and a change in the "purpose" standard in the Patriot Act could be defeated by requirements for minimization. Worse yet, one reading of the FISC decision is that the court attempted to duck the effects of the Patriot Act amendments. While this tactical judgment by the FISC was certainly questionable, the court made plain why it thought the few restrictions it imposed on DOJ were consistent with FISA and were perhaps required by the Fourth Amendment.

On the one hand, the concern exposed by the May 17 FISC opinion is easy to envision after stripping away the technical questions of statu-

111. *Id.*

112. *FISCR Opinion*, 310 F.3d at 730.

113. *Id.* at 625.

114. *FISC Decision*, 218 F. Supp. 2d at 611 ("the proposed . . . procedures eliminate the bright line . . . prohibiting direction and control by prosecutors. . .").

115. For an illustration of the media's immediate response to the FISCR Opinion, *see A Green Light to Spy*, N.Y. TIMES, Nov. 19, 2002, at A30; *Chipping Away at Liberty*, WASH. POST, Nov. 19, 2002, at A24.

tory interpretation: prosecutors may seek to use FISA to end-run the traditional law enforcement warrant procedures. While they understandably gain flexibility that way, they also become less accountable to the Constitution and courts, and anyone in the United States could be subject to surveillance and later arrested and detained without the protections afforded by the criminal justice system. On the other hand, the FISC analysis and subsequent reversal on appeal were unquestionably colored by the recent history of mistrust between the Justice Department and the FISC. The FISC reacted to alleged abuses and inadequate management of FISA activities within the Department. The FISC created a cumbersome set of procedures and monitoring requirements that contributed to the compromise of essential agency coordination among intelligence and law enforcement officials.

V. THE FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW (FISCR) DECISION

Along with its May 17 opinion, the FISC adopted a rule of court procedure that requires all FISA applications to "include informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors."[116] Defying the May 17 order, the government proposed in a new application to the FISC on July 19 to use their proposed March 2002 Procedures without modification.[117] Although the FISC judge granted the application, the order modified the Procedures consistent with the May 17 order.[118] The modification formed the basis for the appeal to the FISCR.[119] On September 9, 2002, the nation's most secret appellate court, the three-judge Foreign Intelligence Surveillance Court of Review (FISCR), met for the first time in its twenty-four year history to consider the first appeal from a decision of the FISC. The three senior status federal judges, appointed as prescribed in FISA on a rotating basis by the Chief Justice, had no experience with FISA or the FISC. Nor had any of them presided over such an explicitly one-sided appeal. As presiding Judge Ralph B. Guy observed, the hearing "is a strange proceeding because it is not adversarial. . . . One might think that the adversary . . . is [the FISC]."[120] The Justice Department confirmed that the hearing took place only after congressional staffers and civil liberties groups complained that they were denied access to or a chance to par-

116. *See FISC Decision*, 218 F. Supp. 2d at 627 (where the Court promulgated Rule 11, Criminal Investigations in FISA Cases).

117. *FISCR Opinion*, 310 F.3d at 730.

118. *Id.*

119. *Id.* at 729-30.

120. Hearing Transcript, *supra* note 102, at 100.

ticipate in the hearing. Only Department representatives and the three judges were present at the hearing, where the government's argument was made by Solicitor General Theodore B. Olson.[121] Obviously struck by the absence of an opposing side, Judge Laurence H. Silberman asked Olson for his view of whether the FISCR should accept amicus briefs from groups supporting the FISC decision.[122] Olson replied "that it's probably good" for the court to receive the briefs.[123]

In an opinion issued on November 18, the unanimous FISCR reversed the *en banc* FISC and held that the restrictions on criminal division use of FISA procedures imposed by the FISC are not required by FISA or the Constitution.[124] I believe that the court misread FISA and the Constitution but minimized the harm its analysis caused by resting its decision on a fallback position of the government, which both leaves room for future compromise and invites reforms. The reversal was hardly surprising given all the forces aligned on one side of this appeal. However, the unfortunate rhetoric of the FISCR opinion, along with some comments made at the appeal hearing by counsel and the judges concerning the government's missing chances to stop terrorism in general, and September 11 in particular, because of its misunderstanding of FISA, obscured two important realities: (1) that there is not considerable difference between what the FISC ordered and what the Justice Department wanted; and (2) FISA remains, at its core, an extraordinary mechanism that permits the government to seek foreign intelligence information. To the extent problems of coordination and cooperation plague the intelligence community in its use of FISA, they are more institutional and cultural than legal. Reforms of the institutional culture would better ensure counterterrorism objectives than stretching the legal safeguards of FISA would.

The very fact of the appeal, along with the selection of Solicitor General Olson to argue for the government, underscores the Department's view that the dispute with the FISC was high-stakes. According to the Department's FISA expert, Associate Deputy Attorney General David Kris,

> [A]t stake is nothing less than our ability to protect this country from foreign spies and terrorists. . . . We need *all* of our best people, intelligence and law enforcement alike, working together to neutralize the threat. In some cases, the best protection is prosecution . . . In other cases . . . another method – such as recruitment – is called for. Sometimes you need to use both methods. But we can't make a

121. Philip Shenon, *Secret Court Weighs Wiretaps*, N.Y. TIMES, Sept. 10, 2002, at A13.
122. Hearing Transcript, *supra* note 102, at 99-100.
123. *Id.* at 67-68. (The briefs were ultimately accepted by the court.)
124. *FISCR Opinion*, 310 F.3d at 719-20.

> rational decision until everyone is allowed to sit down together and brainstorm about what to do.[125]

Kris drew an analogy to medicine:

> When someone has cancer, sometimes the best solution is surgery to cut the tumor out. Other times it's chemotherapy. And in some cases you need both. But who would go to a hospital where the doctors can't sit down and talk to each other about what's best for the patient? That's bad medicine. And that's what we're trying to change.[126]

The rhetoric of Kris's statement first appeals to our base instincts by emphasizing the need for security from horrific acts of terrorists, and then it wraps the security appeal in common sense language of a team working together to provide the best options for the cancer patient. Missing from Kris's statement, however, are two critical points of reference. First, Congress provided for the secretive FISA process as a means to facilitate collection of foreign intelligence information, not for any other purpose. Second, the Fourth Amendment requires a higher threshold than FISA before permitting intrusive surveillance when criminal prosecution is the government's aim. Thus, while the law gets in the way of the government's ideal world, the modest legal barriers erected by FISA and the Constitution do not stand in the way of having "*all* of [the] best people . . . working together."[127] The only limits imposed by FISA and by the now-overturned FISC procedures were prevention of prosecutors from directing a FISA operation and insuring that OIPR could "chaperone" operations where intelligence gathering and criminal prosecution were simultaneous objectives of the surveillance. While some of the details of the chaperone portion of the FISC order may well have been an over-reaction to prior Justice Department misdeeds, its overall direction and control limits unquestionably serve the very core objective of FISA, even as amended by the Patriot Act.

Moreover, Kris's medical treatment analogy misleads. The FISA system in place before November did permit, indeed facilitate, the specialist doctors to consult on how best to treat the patient. But, when the specialists sought to employ the shortcut of FISA surveillance, they had to make sure that the FISA doctor was in charge of initiating and controlling those procedures. They also had to be certain that the OIPR surgeons were included in the discussion when the prosecution doctor decided on surgery.

---

125. *The USA PATRIOT Act In Practice: Shedding Light on the FISA Process: Before the S. Judiciary Comm.*, 107th Congress 2d (2002) (Statement of David Kris, Associate Deputy Attorney General) (emphasis added) [hereinafter Kris Statement].

126. *Id.* (emphasis added).

127. *Id.*

As noted above, the FISC accepted the Department's March 2002 proposed procedures in every respect except one. It agreed that intelligence officials may share virtually any information with law enforcement personnel, indicating that the "team" members are indeed fully informed of each other's activities and leads. What the Justice Department did not get from the FISC was approval for law enforcement personnel to direct and control a FISA investigation. The practical effects of this limited rejection of the proposed procedures are not self-evident, and the Department's objection and the FISCR repudiation of the FISC on this point smacks of overkill. The FISC-imposed "chaperone" requirement caused the Department to complain that it is impractical to insist on OIPR involvement in a fast-paced and often times widely dispersed investigation. Giving Justice the benefit of the doubt on this issue, it is not clear that compromises would be unable to save some form of a useful role for OIPR in overseeing these complex and highly intrusive investigations. Although Kris analogized OIPR to a hospital administrator who would be called in to the cancer consultation between oncologist and surgeon, OIPR is more akin to an ombudsman for the cancer patient, whose job is to make sure that the correct treatment is prescribed.

A. *The FISCR Opinion on "Primary Purpose"*

After prodding by Judge Silberman during the September 9 FISCR hearing, the government prepared a supplemental brief to support an argument that Silberman actually outlined for Solicitor General Olson during the hearing – that FISA never contained any restriction on the government's use of FISA information in criminal prosecutions.[128] Applying this argument would mean that the dozens of courts of appeal decisions that employed some kind of "primary purpose" analysis were, according to Judge Silberman, simply wrong.[129] The hearing transcript suggests that Silberman's tack took Olson and his colleagues by surprise. When the FISCR considered the issue in its opinion, the court acknowledged that the argument was not raised in the FISC, and that Silberman's FISA theory had *never* been advanced before a court or Congress.[130]

Unschooled in FISA and its implementation in practice, the FISCR fell into an analytic trap of its own making. The appeals court reasoned that because FISA defines the targets and information to be sought with

128. *See FISCR Opinion*, 310 F.3d at 721; *see also* Hearing Transcript, *supra* note 102, at 33-34.

129. *FISCR Opinion*, 310 F.3d at 722.

130. *Id.* at 721.

close reference to criminal activity, any use of foreign intelligence information derived from FISA activities, including prosecution, is permitted.[131] The FISCR found it "quite puzzling"[132] that the DOJ had, for about twenty years, read FISA as imposing any limit on obtaining FISA orders if its intent was to prosecute the targets. It is hardly credible that the judges would be puzzled by a practice that had been supported as a bedrock component of FISA by dozens of FISC judges and by Congress for twenty-four years. What the FISCR called "an obvious reading of the statutory language that foreign intelligence information includes evidence of foreign intelligence crimes"[133] was neither a new insight nor probative of the limits on law enforcement's use of FISA.

Judicial decisions before and after the enactment of FISA reflect the common understanding that law enforcement and intelligence gathering interests will often overlap in investigations. The pre-Patriot Act FISA case law limited the use of FISA procedures in law enforcement, based on the language of FISA, the *Truong* decision that shaped the subsequent case law, and the legislative history of FISA. It was not that the courts treated the two categories – intelligence and prosecution – as mutually exclusive. As illustrated by *Truong*, the primary purpose analysis necessarily involved a subjective inquiry into what considerations were driving each investigation, and, therefore, the purpose of employing the technique as well.[134]

Moreover, in construing the case law following *Truong*, the FISCR judges misapprehended what foreign intelligence information is actually used for.[135] That there was no discussion in seminal FISA decisions of how the government would use its foreign intelligence outside prosecution efforts does not mean there is no such use, nor does it mean that the government failed to benefit from what was obtained as intelligence information. The cases cited by the FISCR[136] involved instances where prosecution was sought. However, in many cases, the foreign intelligence obtained through FISA is useful in a programmatic sense, or at least constitutes a piece of a larger mosaic and does not lead to prosecution. Contrary to the FISCR assertion that "criminal prosecution analyti-

131. *Id.*

132. *Id.* at 723.

133. *Id.* at 724.

134. *Id.*

135. *Id.* at 726-27.

136. *Id.* at 726-27 (discussing and analyzing United States v. Megahey, 533 F. Supp. 1180 (E.D.N.Y. 1982), *aff'd sub non* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984); United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982); United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987); United States v. Badia, 827 F.2d 1458 (11th Cir. 1987); United States v. Johnson, 952 F.2d 565 (1st Cir. 1991); United States v. Sarkissian, 841 F.2d 959 (9th Cir. 1988)).

cally cannot be placed in a separate . . . category,"[137] the truth is that the FBI had done exactly that for twenty-four years, under FISA.

What the government called a "false dichotomy"[138] between law enforcement and intelligence is hardly so in working out *the reason or reasons* for seeking FISA surveillance. In practice, the FBI has managed that dichotomy as well as can be expected under circumstances where the reasons for intelligence gathering are multiple, mixed, and ever-changing. The fact that the interests and uses blur and merge does not relieve the government of its obligation to comply with FISA. FISCR did not appreciate that the courts that have reviewed criminal convictions where FISA supplied evidence for the prosecution have not concluded that some involvement of law enforcement personnel in a FISA intelligence investigation negated the intelligence purpose of the investigation. The courts further failed to realize that the dual intelligence and law enforcement roles of some FBI agents involved in FISA surveillance resulted in the exclusion of evidence in subsequent criminal prosecutions. In reversing the FISC decision, the FISCR simply missed the mark when it conflated the way FISA information is *used* with *the purpose* for using FISA.

According to the FISCR, evolving interpretations of the 1995 Procedures and the "directing or controlling" language that constrained personnel within the Department of Justice and perhaps specifically within OIPR "prevented the Criminal Division from providing any meaningful advice to the FBI."[139] Those unfortunate interpretations of the Procedures may indeed have seriously impeded FISA counterterrorism investigations before the Patriot Act. The Procedures themselves, however, permitted very broad prosecution/intelligence cooperation and consultation and drew a line only in the most extreme cases – where the Criminal Division would initiate or take over a FISA investigation.

B. *The FISCR on Minimization*

The FISCR complained that the FISC opinion "does not clearly set forth the basis for its decision."[140] Unfortunately, the decision of the FISC judges to review the proposed Justice Department procedures against the FISA minimization requirements confused the FISCR, and the failure of the FISC to respond directly to the Patriot Act amendments provided a relatively easy path toward the FISCR reversal. It is more

137. *FISCR Opinion*, 310 F. 3d at 727.

138. *Id.* at 725.

139. *Id.* at 728 (paraphrasing the FINAL REPORT OF THE ATTORNEY GENERAL'S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NATIONAL LABORATORY INVESTIGATION 721-34 (May 2000)).

140. *FISCR Opinion*, 310 F.3d at 721.

accurate to say that the FISC relied on its interpretation of the FISA minimization requirements for its decision and rejected in part the DOJ procedures as falling short of what FISA demands.

The FISCR correctly observed that minimization procedures are designed to protect against the collection and dissemination of nonpublic information. The rights-sensitive objective of minimization is apparently what prompted the FISC to characterize its information-sharing rules as minimization procedures. However, the FISCR wrongly concluded that FISA requires minimization only of information that is not foreign intelligence information.[141]

The minimization section of FISA contains three provisos. The first is generic and requires

> specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning nonconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.[142]

The second applies to information "which is not foreign intelligence information,"[143] while the third exempts from the first and second set of requirements "information that is evidence of a crime . . . that is to be retained or disseminated for law enforcement purposes."[144] The plain meaning of the first proviso – non-publicly available "information" – expressly covers foreign intelligence information. Thus, it is incorrect for the FISCR to say "there is simply no basis for the FISA court's reliance" on minimization to limit prosecutors' ability to "advise FBI intelligence officials on the initiation, operation, continuation, or expansion of FISA surveillances to obtain foreign intelligence information."[145] Minimization may have not been the best vehicle for dealing with the law enforcement/intelligence overlap, particularly after the Patriot Act, but it is at least an understandable analysis, and defensible.

C. *The FISCR and "Significant Purpose"*

By misunderstanding the minimization requirements of FISA, the FISCR got off on the wrong foot. Much of the controversy surrounding the "wall," as noted previously, is based on what the Department of Justice, and later the FISCR, characterized as a false dichotomy between

141. *Id.* at 731.
142. 50 U.S.C. § 1801(h)(1) (2000).
143. *Id.* § 1801(h)(2).
144. *Id.* § 1801(h)(3).
145. *FISCR Opinion*, 310 F.3d at 731.

a foreign intelligence purpose and a law enforcement purpose. In one sense, there is no dichotomy between law enforcement and collection of foreign intelligence as FISA objectives. By FISA definition, the collection of foreign intelligence concerning U.S. persons involves looking for information where it is thought that some sort of national security crime may occur.[146] It has also been clear, since the enactment of FISA in 1978, that "foreign intelligence information" may be evidence of a crime that could be used in the prosecution of a national security crime.[147] Regarding the intended purpose of the surveillance or search that is requested pursuant to FISA since 1978, however, there has been, and remains today, a dichotomy between law enforcement and intelligence. Since 1978, the FISA mechanisms are available *only* when the purpose (or, after enactment of the Patriot Act, a "significant purpose") of the surveillance, for which FISC permission is sought, is to gather foreign intelligence, even though the information collected may include evidence of a crime and that such evidence could be used later in a criminal prosecution.

The FISCR recognized that the new DOJ argument prompted by Judge Silberman's questions during the appeal hearing was at odds with its "significant purpose" argument. The court thus backed down slightly from its first conclusion (that FISA should never have been read to limit prosecution objectives) and decided that "the better reading" of FISA as amended is to "exclude from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution."[148] The court then stated that there is little practical difference between these interpretations in most instances, so long as the government has not unequivocally decided when an application to prosecute is made under FISA, and "a realistic option" remains for dealing with the target in some other manner.[149] The court concluded that if "the government's sole objective was merely to gain evidence of past criminal conduct – even foreign intelligence crimes – to punish the agent . . . the application should be denied."[150]

The change to "significant" purpose adopted in the Patriot Act altered the balance in deciding whether to approve an application for FISA surveillance or search. So long as a significant purpose of the surveillance or search is to gather foreign intelligence, law enforcement aims may also shape the request to the FISC. The Justice Department maintained that the "significant" purpose amendment to FISA would

146. *See* 50 U.S.C. § 1801(e) (2001) (linking information sought and criminal conduct).
147. *Id.*
148. *Id.* at 735.
149. *Id.*
150. *Id.*

affect a very small subset of cases, those where the target is an agent of a foreign power and is committing an unrelated crime.[151] One example could be where an international terrorist is also a drug dealer — not to support terrorist activities but to support himself. Gathering evidence for a drug prosecution could not be the sole purpose of a FISA search. But the government's position is based on a false premise. It fails to recognize that seeking FISA surveillance of even a known agent of a foreign power for the purpose of prosecuting a crime related to terrorism (such as where drug dealing was used to fund terrorist activities) is also subject to the "significant purpose" rule.

Although the Patriot Act did lower the wall between intelligence and law enforcement, that wall was not removed, and the essence of FISA as an exceptional procedure for the gathering of foreign intelligence information remains. Each of the statutory definitions of "foreign intelligence information" pertains to a category of intelligence that may further the counterterrorism goals of law enforcement, but each definition also requires that the surveillance be for "information" that furthers these purposes. Obtaining "evidence for conviction" is different from obtaining "foreign intelligence information," even if the conviction will deter terrorism. Although "foreign intelligence information" has always included information that could be evidence of a crime, seeking that information *in order to prosecute* is not the same as seeking that information in order to prevent possible terrorist activities. A proper reading of FISA reveals that the Criminal Division may not direct and control a FISA investigation where the only objective is to prosecute the target.

The Department maintained in its brief that the "foreign intelligence" definition does not limit how the government *uses* the information it obtains to achieve the protections sought by FISA.[152] Protection against the threats listed in FISA may be achieved in many ways, including by prosecuting the alleged terrorist or spy. This assertion is true, so long as the surveillance or search is lawful at the outset. Only if there is a significant foreign intelligence purpose, certified by someone with national security responsibility at the Justice Department, can the information obtained be used later in a prosecution.

The most controversial issues do not concern consultation and advice, but instead involve instances where the Criminal Division seeks to initiate or direct an investigation *in order to prosecute*. The "direction and control" approach created by the FISC was designed to preserve the underlying purpose of FISA – to collect foreign intelligence infor-

151. Kris Statement, *supra* note 125, at 7.

152. Brief for the United States at 14, In re Sealed Case Nos. 02-001, 02-002, 310 F.3d 717 (U.S. Foreign Intell. Surveil. Ct. Rev. 2002) (No.02-001) [hereinafter DOJ Brief].

mation from agents of a foreign power in order to protect the United States from terrorism and espionage threats. Like the "chaperone" requirement, the direction and control limit supplies a prophylactic against a prosecutor's making use of FISA *in order to build* a criminal case.

The FISCR opinion is thus internally inconsistent. The court first concluded that FISA never limited the use of foreign intelligence for law enforcement purposes. Then it maintained that the Patriot Act amendment imposes such a limit, albeit a lesser one than that which the court says never existed! The court's opinion admitted that the Patriot Act eliminated the "primary purpose" approach that the Justice Department, the FISC, and all other Article III courts had been using to review alleged misuses of FISA surveillance since pre-FISA days.

The FISCR did not specifically relate this unrecognized concession to its conclusion that even "direction and control" can properly be in the Criminal Division's hands. Apparently, the direction and control authority could not be exercised if the "sole objective" is prosecution. However, in a given situation, the government may fully intend to prosecute a spy or terrorist, but at the same time need to know with whom he is involved, precisely what he has done, whether others are complicit, and whether he or his co-conspirators can be "turned." Thus, there may be a logical and lawful time for the prosecutor to control the nature of the FISA targeting because the prosecution may have to be structured in such a way that the government can avoid giving notice that FISA surveillance was conducted.

Finally, the FISCR compounded its misapprehension of FISA when it declared that the FISC has no authority to "inquire into which Justice Department officials were instigators of an investigation" in reviewing a certification under FISA.[153] The FISCR also charged that, in making such an inquiry, the FISC "may well have exceeded the constitutional bounds that restrict an Article III court" by telling the Department of Justice "how to deploy personnel resources,"[154] a function reserved by the Constitution to the Executive or to Congress.[155] However, as the former Counsel for Intelligence Policy testified in Senate hearings in September 2002, regardless of the "purpose" language, the FISA requirement that an official "employed in the area of national security"[156] make the certification underscores that FISA surveillance was to be undertaken only when a national security objective for the surveil-

153. *FISCR Opinion*, 310 F.3d at 736.

154. *Id.* at 731.

155. *Id.*

156. 50 U.S.C. §§ 1804(a)(7)(A-B) (2000).

lance is present.[157] Contrary to the FISCR assertion that "[t]here is nothing in FISA or the Patriot Act that suggests otherwise,"[158] FISA further underscores the intelligence gathering purpose of these special authorities by insisting that a national security official, not a prosecutor or criminal investigator, make the relevant certification. The FISA assignment is ministerial, prescribed by Congress, not the FISC. FISA clearly supplies the legal authority for making the ultimate certification decisions.

D. *The FISCR and the Fourth Amendment*

The FISCR characterized the FISC decision as reflecting the opinion that "Title III procedures are constitutionally mandated if the government has a prosecutorial objective regarding an agent of a foreign power."[159] This characterization is not quite correct. The FISC would remit the government to Title III if it were seeking to employ FISA when its only objective was to build a criminal case.

The Department of Justice brief inaccurately characterized the *Keith* decision as drawing the constitutional boundaries for surveillance on the basis of the "nature of the threat, not the nature of the government's response to that threat."[160] In fact, both elements figured in *Keith's* balancing formula. The Supreme Court recognized that different standards might be constitutional "if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[161] The Court emphasized that the government's duty to protect the national security was pitted against the danger that unmonitored executive surveillance would abuse individual rights.

The *Keith* Court supported an exception to the warrant requirement because it may be "reasonable" under the Fourth Amendment to use other procedures in pursuit of intelligence information.[162] FISA occupied the exception recognized by the Supreme Court, leaving the law enforcement model in place. FISA did not negate the warrant requirement itself. Although it is common to refer to what the FISC issues as "warrants," they have that label not because they are Fourth Amendment warrants, but rather because the FISC permits the type of surveillance

157. *See The Delicate – and Difficult – Balance of Intelligence and Criminal Prosecution Interests in the Foreign Intelligence Surveillance Act, Before the Senate Judiciary Comm.* (Sept. 10, 2002) *available at* 2002 WL 31013657 (statement of Kenneth C. Bass, III).

158. *FISCR Opinion*, 310 F.3d at 736.

159. *Id.* at 737.

160. DOJ Brief, *supra* note 152.

161. *Keith*, 407 U.S. at 322-23.

162. *See* Banks & Bowman, *supra* note 95, at 52.

associated with a Title III warrant. Left to its own devices, the government might invoke the unprecedented "war on terrorism" and permit the national security exception to serve the purpose of gathering evidence for conviction, collapsing the careful distinction endorsed by the Court in *Keith*. Allowing the government to employ FISA when the sole objective is to enforce the criminal laws, however, would be unconstitutional, in violation of Fourth Amendment protections.

The FISCR compared Title III and FISA thresholds and procedures and asserted that the differences are not constitutionally significant. To say that the statutes differ to some extent in their probable cause showings seriously understates those differences, as the FISC decision made clear. The Court ignored the fact that FISA surveillance and searches may be constitutionally reasonable precisely because they are available when the government is collecting information for foreign intelligence purposes. The FISCR conclusion that FISA may not be employed if the sole objective of the surveillance or search is prosecution means that the FISA/Title III distinction must be observed at least in those instances. Arguably, the same analysis should govern an ongoing investigation, meaning that when the Justice Department determines that the only reason to continue FISA surveillance is to prosecute, Title III procedures should be followed.

The FISCR conclusion that the amended FISA satisfies the Fourth Amendment's reasonableness requirement is itself tenable only if FISA is construed to forbid the Criminal Division from using FISA to engineer prosecution. Applying the traditional canon of constitutional avoidance, the narrow construction should be applied to save the statute's constitutionality. FISA should not be used simply *in order to prosecute*, but its procedures may be used to obtain foreign intelligence in circumstances where Title III might not be a practical alternative. In such situations, the prosecutor participates in FISA in order to enhance the entire government's options, not merely those of the Criminal Division.

The government brief to the FISCR argued that, before the Patriot Act, federal courts treated law enforcement and intelligence gathering purposes "as if the two terms are mutually exclusive."[163] The historical record belies this assertion. Far from separating the two, the "primary purpose" standard recognized the frequent overlap of law enforcement and intelligence operations, and sought to draw a reasonable line to guide law enforcement and intelligence officials as they manage parallel investigations.[164]

---

163. DOJ Brief, *supra* note 152, at 20.

164. *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980); United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

Picking up on the government's argument, the FISCR accused the *Truong* court of drawing a line between intelligence and law enforcement that "was inherently unstable, unrealistic, and confusing."[165] Admittedly, this pre-FISA decision could not have foreseen the growing threat of terrorism and the necessary merging of intelligence and law enforcement interests in combating terrorism. The court's *Troung* analysis was "unstable" in that respect. Yet in FISA, Congress soon supplied the necessary stability to manage the overlap and thus greatly affected the Fourth Amendment calculus.

It was never true, as the FISCR said it might have been when *Truong* was decided, that "foreign policy concerns recede"[166] once the prosecution interests become dominant.[167] Still, the *Truong* approach had not otherwise proven unworkable until it was changed by Congress through the Patriot Act. In fact, the organizational division of the Justice Department into criminal and intelligence compartments helped the reviewing court determine the purpose of the surveillance or search. It also served the same end for the FISC, and worked reasonably well within the Department to maintain a wall when one was needed. To the extent that the information sharing broke down, the legal standard was not the cause. Contrary to the FISCR assertion that the "primary purpose" standard may itself be "dangerous to national security" because it "punishes . . . cooperation,"[168] the existing standard protected Fourth Amendment interests while it provided a workable framework for cooperation among intelligence and law enforcement officials.

Even though arresting or prosecuting a potential terrorist "may well be the best technique"[169] for attaining the prevention goals of the intelligence community, it is not determinative of the procedures that must be followed before the surveillance or search is conducted. Government agents may well be in pursuit of "foreign intelligence information" as defined in FISA, the target may be an "agent of a foreign power," and the information sought may concern "international terrorism" as defined in FISA. But, if the Criminal Division is setting out to prosecute, FISA may not be used *unless* (following the Patriot Act) there is also a "significant" intelligence gathering purpose. The procedures in FISA and Title III are different for two important reasons: First, the higher stakes for the target of law enforcement investigations merit greater assurance that the investigators are close to nabbing criminals, and second, the imprecision and long-term nature of preventive intelligence gathering, where

165. *FISCR Opinion*, 310 F.3d at 743.
166. *Truong*, 629 F.2d at 915.
167. *FISCR Opinion*, 310 F.3d at 743.
168. *Id.*
169. *Id.* at 724.

targets are often not identifiable by the government in advance of surveillance, suggest different considerations in reviewing an application for surveillance. Government agents must select the "best technique" with these constraints in mind.

Finally, the FISCR analogized the revised FISA to situations where the Supreme Court has approved warrantless searches that were designed to meet the government's "special needs, beyond the normal need for law enforcement."[170] However, the analogy fails for the same reason that the FISCR's efforts to minimize the differences between Title III and FISA procedures come up short: the "special needs" cases –searches for drugs in the school lockers, or immigration checkpoints at the nation's borders – are not primarily concerned with law enforcement objectives. Nor is FISA a law enforcement tool, and the Supreme Court's "special needs" cases cut against, rather than for, the FISCR analysis of FISA.

In the end, the FISCR concluded that FISA searches are constitutionally reasonable, and that they must meet the balancing test from *Keith*.[171] What the FISCR failed to acknowledge is that the few constraints imposed by the FISC on Justice Department operations concern law enforcement operations that use FISA to avoid Title III. Only the chaperone rule appears to have the potential to compromise effective cooperation and information sharing. In this limited context, surely the Justice Department and the FISC could develop a better arrangement.

E. *A Failed Attempt to Obtain Supreme Court Review*

In the latest twist in this remarkable tale, public interest groups led by the American Civil Liberties Union (ACLU) filed a petition for leave to intervene and a petition for a writ of certiorari to the Supreme Court.[172] However, the ACLU acknowledged that FISA authorizes Supreme Court review only upon petition by the government following the denial of a government application by the FISCR.[173] Until now, of course, there has been no petition filed for Supreme Court review because the government has never before appealed to the FISCR, much less to the Supreme Court. To obtain Supreme Court review under FISA, the public interest groups had to overcome two difficult legal

170. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995).

171. *FISCR Opinion*, 310 F.3d at 746.

172. The names of the other interveners include the National Association of Criminal Defense Lawyers, American-Arab Anti-Discrimination Committee, and Arab Community Center for Economic and Social Services. *See* David L. Hudson Jr., *Unusual Ruling Leads to Unusual Filing: ACLU Asks U.S. Supreme Court to Review Intelligence Court's First Rescission*, ABA J. REP., Feb. 28, 2003.

173. 50 U.S.C. § 1803(b) (2000).

problems: (1) they were not parties to the proceedings in the FISC or the FISCR and had no right to such status; and (2) the government position was supported, not denied, by the FISCR. The ACLU petition interpreted FISA's jurisdiction provision as reflecting only congressional silence on Supreme Court review in these circumstances. In addition, it interprets FISA as supporting an intention that the Court should correct the FISCR when it makes a mistake.[174] Failing jurisdiction under FISA, the interveners argued that the general authority to seek a writ of certiorari from a court of appeals[175] supports their claim, as does the All Writs Act.[176] Even if their statutory arguments succeeded, however, the interveners also had to satisfy the Article III standing to sue requirements. To meet this hurdle, the groups argued that they have associational standing to represent their members because the members have suffered actual or threatened injury from unlawful FISA surveillance.[177]

On the merits, the interveners argued that the FISCR should and could have successfully avoided deciding the constitutionality of the Patriot Act amendments to FISA by narrowly construing FISA to forbid FISA orders when law enforcement is the primary purpose of the surveillance or search. Otherwise, they urge the Court to "make clear that the government may not constitutionally rely on any foreign intelligence exception to the Fourth Amendment's usual requirements in investigations whose primary purpose is law enforcement rather than foreign intelligence."[178] According to these groups, decisions of such importance "should not be finally adjudicated by courts that sit in secret, do not ordinarily publish their decisions, and allow only the government to appear before them."[179] On March 24, 2003, the Supreme Court dismissed the petition.[180]

F. *Useful Reforms*

Congress should undertake a comprehensive review of FISA and its role in counterterrorism and homeland security. Between its enactment in 1978 and the amendment to permit physical searches using FISA in 1994, the statute remained unchanged. Since the mid-1990s, however,

174. *See* American Civil Liberties Union, et al. Petition for Leave to Intervene and Petition for a Writ of Certiorari, *In re* Sealed Case of the Foreign Intelligence Surveillance Court of Review, 310 F.3d 717 (FISCR 2002) (No. 02-001) [hereinafter ACLU Petition].

175. 28 U.S.C. § 1254 (2000).

176. *Id.* § 1651(a).

177. *See* ACLU Petition, *supra* note 174.

178. *Id.*

179. *Id.*

180. Am. Civil Liberties Union v. United States, 123 S. Ct. 1615 (2003); *see also* Linda Greenhouse, *Opponents Lose Challenge to Government's Broader Use of Wiretaps to Fight Terrorism*, N.Y. TIMES, Mar. 25, 2003, at A12.

piecemeal changes to FISA have been added, often without careful consideration of the effect of the new provisions on existing law. Some of this has arisen from the rush to match developments in technology and in terrorists' techniques for evading detection. The Patriot Act reforms are only the most prominent examples.[181] In light of the construction given the Act both by the Department of Justice and the FISCR, Congress should rethink the "significant purpose" change, and should examine again the information sharing mechanisms it authorized. Senator Patrick Leahy opined that, if the government wishes to employ FISA procedures for law enforcement purposes, maybe FISA should be amended to incorporate Title III standards.[182] Alternatively, Congress could simply return to the "purpose" language of 1978, or it could codify the FISC procedures to forbid that the prosecutors direct and control a FISA investigation. Whatever the form of the correction, one is needed. Congress should step up to the challenge of a comprehensive reconsideration of FISA and its objectives. Because the portions of the Patriot Act at issue in this dispute are set to expire on December 31, 2005,[183] the opportunity for reform and reconsideration of Patriot Act measures is particularly compelling.

In a February 2003 report,[184] Senate Judiciary Committee members Leahy, Grassley, and Specter lamented what they characterized as a series of FISA implementation failures by the FBI. They asserted that FBI and Justice Department officials were setting "too high a standard to establish that there is 'probable cause' that a person may be an 'agent of a foreign power'" and, therefore, too high a standard for obtaining surveillance pursuant to FISA.[185] The "probable cause" question is one that merits serious legislative deliberation. There is nothing in the text of FISA, very little in its legislative history,[186] and nothing in any of the case law reviewing FISA surveillance that comments on whether the different predicates (foreign agency and criminal conduct) in FISA and Title III imply different "probable cause" standards in the two settings.

---

181. Amendments to FISA enacted in 1998 allow the government to install pen registers and trap and trace devices (*see* 50 U.S.C. §§ 1841-1846), and to gain access to business records (§§ 1861-1862). Changes made in 1999 expanded FISA's definition of "agent of a foreign power" (§ 1801(b)(2)(D)).

182. Senator Patrick Leahy, Chairman, Comm. on Judiciary, *The USA PATRIOT Act in Practice: Shedding Light on the FISA Process,* (Sept. 10, 2002) [hereinafter Leahy], *available at* http://leahy.senate.gov/press/200209/091002.html.

183. USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). (Specific Provision?)

184. Interim Report, *supra* note 78.

185. *Id.* at 12.

186. *See* S. REP. No. 95-604 at 47 (1978) ("In determining whether probable cause exists under this section, the court must consider the same requisite elements which govern such determinations in the traditional criminal context.").

This term of art may mean the same thing in both settings. If so, the phrase has been defined by the Supreme Court in *Illinois v. Gates*[187] as requiring an examination of "the totality of the circumstances," including the veracity and basis of knowledge of persons supplying hearsay information "that there is a fair probability" that the criminal conduct is occurring.[188] The Gates Court concluded that "probability" based on the "totality of the circumstances" was preferable to a "preponderance of the evidence" standard.[189] At a minimum, the part of the *Gates* standard requiring "that the criminal conduct is occurring" should not apply because no criminal occurrence is required to obtain a FISA order. Otherwise FISA probable cause may involve the same factual inquiry as in law enforcement investigations, subject to the possibility that Congress may anticipate a lesser factual predicate when foreign intelligence information is sought.

Among the more specific reforms to FISA that Congress could consider would be a formal role for the FISC in reviewing and approving FISA guidelines, akin to the role the Supreme Court assumes in reviewing the Rules of Civil Procedure and Rules of Evidence. Moreover, the appeal of the FISC decision lays bare the one-sided nature of FISA proceedings. Congress should consider an amendment to FISA that permits the creation of a list of security-cleared counsel who could brief and argue any subsequent appeals from the FISC. In the weeks after the FISCR decision, a leaked draft of proposed legislation in the Justice Department included such a proposal.[190]

A proposed Patriot Act II has been widely circulated on the internet recently. Although many of its provisions constitute the remains of what was dropped from the 2001 Patriot Act, some of the proposals are new. Of those that pertain to FISA, the most prominent include a carry-over from the last Congress that would permit FISA procedures to be used in investigations of "lone wolf" terrorists, eliminating the requirement of foreign agency.[191] Other provisions would expand the definitions of "agent of a foreign power" to reach those for whom no criminal activities are shown,[192] expand the list of Department of Justice officials who could authorize the use of FISA-obtained information by law enforce-

187. 462 U.S. 213 (1983).

188. *Id. at* 236, 238.

189. *Id.* at 238.

190. *See* Draft Version of Domestic Security Enhancement Act of 2003 ("Patriot Act II") § 108, *available at* http://www.dailyrotten.com/source.docs/patriot2draft.html.

191. *See id.* § 101.

192. *See id.* § 102.

ment,[193] lessen the requirements for obtaining FISA pen registers,[194] and expand the wartime exception to the FISA warrant requirement.[195]

VI. A FINAL ASSESSMENT: WHERE THINGS STAND NOW

The government has proudly showcased what it views as some important successes in the war against terrorism purportedly as a result of the expanded authorities granted in the Patriot Act. For example, in February 2003, federal prosecutors brought racketeering charges against a Florida professor and seven others, based on allegations that they financed suicide bombings in Israel.[196] At a televised news conference, the Attorney General stated that the indictment relied heavily on expanded powers granted the Department after September 11. Department officials told the New York Times that prosecutors "were stymied" earlier by restrictions that previously limited the use of foreign intelligence information in criminal cases. Prosecutors maintained that much of the intelligence central to the indictment was only recently made available to them, though much of the material is ten years old. According to the Department, changes in the law made by the Patriot Act in October 2001 broke this logjam and permitted the prosecution to move toward an indictment in this important case.

The FBI began investigating Sami Al-Arian, the principal defendant, in the early 1990s and sought and received permission to conduct electronic surveillance of his conversations pursuant to FISA. Under FISA, officials had the capacity to bug Al-Arian's conversations without ever informing him that he was under surveillance. They also had the power to obtain permission for the surveillance without demonstrating that Al-Arian was committing or about to commit a crime.[197] Over time, the surveillance revealed evidence that Al-Arian and his co-defendants were involved in raising money for suicide bombings and for the families of suicide "martyrs" killed in their terrorist attacks.

The implication of the news conference and attendant media coverage was that before October 2001 the government was restricted legally from doing what it needed in order to build a criminal case against these alleged supporters of terrorism against Israel.[198] Neither the implied

193. *See id.* § 105

194. *See id.* § 107.

195. *See id.* § 103.

196. Eric Lichtblau & Judith Miller, *Indictment Ties U.S. Professor to Terror Group*, N.Y. TIMES, Feb. 21, 2003, at A1.

197. *See* 50 U.S.C. § 1801(b)(2)(C) (2003). Because Al-Arian is a United States person, officials were required to associate him with national security crimes in order to obtain permission for FISA surveillance.

198. *Id.*

message, nor the Attorney General's statements hold water. To be sure, the case against Al-Arian and his co-defendants is heavily laden with foreign intelligence information, much of it derived from surveillance conducted under FISA. However, before and after the Patriot Act, FISA permitted foreign intelligence information to be used in criminal prosecutions so long as investigators sought the FISA surveillance for foreign intelligence purposes. Nothing suggests that the Department ran afoul of that limitation in FISA, nor that FISA or any other law limited the sharing of information between the intelligence and law enforcement officials working on the case. The delay was more likely attributable to the massive number of documents involved in the surveillance operation, many not translated. In addition, there were possible differences between the Justice Department and the U.S. Attorney's Office on how to proceed in the case.

Furthermore, the dramatic public spectacle of a never-before-convened secret court of appeals rebuking all of the judges of a twenty-five year old secret court may be best understood as a product of the highly charged security climate in which the dispute arose. The Patriot Act became law within a few weeks of September 11, 2001. The Act was the result of a remarkable campaign by the Attorney General and his lieutenants to push through Congress a massive, complex, and controversial set of reforms designed to enhance national security. Inevitably, typical deliberation in Congress was shortchanged as members jumped "on board" the war against terrorism. Staff work was rushed, interested groups had little time to prepare or to participate in the debates, hearings were curtailed, and committee reports were perfunctory at best. As Solicitor General Olson remarked before the FISCR in commenting on the meaning of the Patriot Act amendments to FISA, "we're not dealing with perfect clarity here."[199] Although the government marshaled the usual persuasive series of comments from key members of Congress indicating that they understood that the change in FISA to "significant" purpose would lower the barrier to the use of FISA procedures for law enforcement,[200] the scant legislative history lacks any indication that members or Congress as a whole considered the effect of the amendments on FISA as a whole. In fact, the 1977-78 legislative history still forms the major corpus of the rationale for and purposes of FISA, and it continues to speak resoundingly about gathering foreign intelligence. Moreover, the tinkering to FISA that was done in the Patriot Act failed to change the specific requirement that an official employed in the area

199. Hearing Transcript, *supra* note 102, at 55.

200. *See FISCR Opinion*, 310 F. 3d at 732-33 (discussing Patriot Act legislative history).

of national security make the certification that the FISA predicates have been met.

Despite this truncated legislative process, the FISC and the FISCR still had to interpret the law that was before them. The plain meaning of the change in purpose favors permitting more involvement of the Criminal Division in FISA investigations. However, the purpose language combined with the new information-sharing authority still does not sanction the Criminal Division's directing and controlling the FISA activities. If simple textual interpretation and the Patriot Act legislative history leave any doubt on that issue, the underlying twenty-five year old FISA understanding that the overriding objective of the special procedures is to permit the secret gathering of foreign intelligence information supports the FISC-approved procedures. This notion is based on the rule of statutory interpretation disfavoring repeals by implication.[201]

Looking back at the FISC and FISCR decisions, it is safe to say that the rhetoric of crisis and fear seemed to outstrip calm reflection in resolving this dispute. It was well known to all attendees at the FISCR hearing that Solicitor General Olson suffered personally, as his wife was a September 11 victim. While Olson's professionalism and skills as an advocate are beyond reproach, his characterization of the FISC procedures as making it "difficult for us to prevent another September 11"[202] while treating criminal prosecutors "as typhoid Marys"[203] who "have one or two hands tied behind [their] back"[204] did not contribute to reasoned debate. Like others in the Department, FISA novice Olson characterized the purpose requirement as reflecting the need "to collect information to protect the public and to protect the Republic."[205] While this principle is lofty and idealistic, FISA is much more specific in defining its objectives. Likewise, Olson also conflated in his argument the uses of FISA information and the purpose for which it is sought.[206]

The FISCR opinion did not escape the aura of September 11. At one point, the court noted the suggestion that pre-Patriot Act FISA rules "whether correctly understood or not" may have led to missed opportunities by the FBI to anticipate September 11.[207] Although the court cautioned that September 11 does not mean "that we should be prepared to

201. *See* William C. Banks & Peter Raven-Hansen, *Pulling the Purse Strings of the Commander in Chief*, 80 VA. L. REV. 844, 855-56 (1994); *see also* Hearing Transcript, supra note 102, at 58.

202. Hearing Transcript, *supra* note 102, at 63.

203. *Id.* at 17-18.

204. *Id.* at 23.

205. *Id.* at 39.

206. *Id.* at 8-9.

207. *FISCR Opinion*, 310 F.3d at 744.

jettison Fourth Amendment requirements in the interest of national security,"[208] its order that the FISC abandon its limits on the government's FISA applications threatens to do just that.

At one level, the entire episode of the FISC decision and subsequent reversal by the FISCR made the proverbial mountain out of the molehill and overstated the differences between the Department of Justice and the FISC. Once Congress acceded to the administration's proposal to change the purpose language in FISA in the weeks after September 11, there may be few actual instances when a "significant" foreign intelligence purpose cannot be described to accompany a request to the FISC under FISA that is otherwise seeking to build a national security criminal case. The difference between forbidding a law enforcement role in "directing and controlling" under the FISC 1995 Procedures and having the Criminal Division involved in the initiation, operation, continuation, or expansion of future FISA activities may be material in only a handful of cases.

As I have argued, the FISC was almost surely correct in its interpretation of the overriding foreign intelligence gathering purpose of FISA, though it was ill-served by its characterization of the intelligence/law enforcement overlap as one merely involving minimization. Likewise, the FISCR was almost surely on firm ground in rebuking the FISC for not responding to the Patriot Act arguments advanced by the government, but it was amateurish in its characterization of FISA and its aims, and heavy-handed in its disregard for twenty-five years of FISA history. All of this came from an appeals court that had never before met and that reversed an *en banc* FISC, where all seven members had considerable experience in administering FISA. Finally, the FISC was on solid ground in prescribing an OIPR monitoring role to manage the intelligence/law enforcement overlap. However, the "chaperone" rule that emerged may have been too cumbersome to be workable. Compromise could surely have been reached had the FISCR not erred in unfamiliar territory.

The appeal was a one-sided affair. No surveillance target had had his application for surveillance rejected below; although, if such a denial had occurred, then the target would nonetheless not have been aware of the denial or any appeal, and would not have been represented in any FISA proceeding. Hence, the appeal was not adversarial in any respect.[209] The FISC was not represented on appeal, and only Department of Justice personnel were permitted to join the FISCR in the hear-

208. *Id.*

209. *Id.* at 721 n.6 (The court noted that the *ex parte* nature of its proceedings allowed it to entertain arguments for the government not presented to the FISC).

ing room to witness the argument. Although the FISCR agreed to accept and to consider amicus briefs after the hearing,[210] the *amici* could not be and were not well informed about the internal procedures for managing FISA, and their briefs focused primarily on the Fourth Amendment issues.[211]

As construed by the FISCR, the Patriot Act change to permit FISA surveillance or searches if there is a "significant" foreign intelligence purpose is potentially unconstitutional. As the FISC noted, prosecutors unburdened by the 1995 FISC minimization procedures may initiate or take over an investigation using FISA procedures when they lack Title III or Rule 41 probable cause, and without notice to the target or affording an adversarial discovery of the FISA applications and orders.[212] If FISA procedures are followed *in order to prosecute*, the exception to the warrant clause impliedly accepted by the Supreme Court in *Keith* does not apply, and the Fourth Amendment requires a law enforcement warrant before the search or surveillance. Only a narrow reading of the significant purpose requirement, within the larger foreign intelligence framework of FISA, can save its constitutionality.

Apart from the issue of its constitutionality, the Patriot Act change to "significant" purpose may have been ill-advised, as recognized by several members of Congress during 2002 hearings.[213] However, the impetus for the change was to permit information sharing, not the direction and control of FISA surveillance and searches by the criminal division. The FISCR resorted to dictionaries to support its conclusion that "consult" includes giving advice.[214] But the critical activity is not advice-giving, but rather direction and control. It is not persuasive to assert, as the FISCR does, that authorizing consultation and coordination (the aim of the Patriot Act changes) implies that either prosecutors or intelligence officials "could be taking the lead" because no express limit was included in the Act on direction or control.[215] Sharing information through consultation and coordination is not the same as running the show. FISA requires that a national security official make the certification in every case. Intelligence officials would normally take the lead; the Criminal Division could do so only when a significant intelligence purpose remains.

---

210. Hearing Transcript, *supra* note 102, at 67-68.

211. *See* ACLU Petition, *supra* note 174, at 24-36.

212. *FISC Decision*, 218 F. Supp. 2d at 624.

213. *See, e.g.*, Leahy, *supra* note 181 (emphasizing that the Patriot Act "sought to amend FISA to make it a better foreign intelligence tool. But it was not the intent of [the Act] to fundamentally change FISA from a foreign intelligence tool into a criminal law enforcement tool.").

214. *FISCR Opinion*, 310 F.3d at 733-34.

215. *Id.* at 734.

Throughout its analysis of FISA, the FISCR was disadvantaged by any effective representation of the FISC and its views on appeal. The characterization of the FISC decision as misapplying minimization procedures illustrates that the FISCR seized a possibly ill-framed portion of the FISC opinion to make a broader charge. The court claimed that the FISC was using minimization to control the dissemination of FISA information even to FBI agents. A careful reading of the FISC opinion reveals no such attempt. On the contrary, the FISC limited the Justice Department only in those instances where prosecutors would attempt to direct and control surveillance, where, in effect, the Justice Department would employ FISA to run around the stricter requirements of Title III. In addition, FISCR failed to grasp that any fencing in of FBI agents in the Criminal Division was more likely the result of the institutional culture of the agency than of any rules imposed by the FISC. It may be, however, that the practical effect of the FISC ruling as seen inside the government was to prevent the intelligence agent from talking to the criminal agent who was focused on the same subject or a related subject.

The impetus to tear down the wall is understandable. Cooperation and coordination are markers for good government. However, aside from the constitutional rights issues that stand in the way of prosecutors' taking charge of the secretive FISA process, there are reasons to suspect that the wall actually has had positive net effects. The FBI National Security and Criminal divisions traditionally have sought different kinds of information, for different purposes. The natural rivalry between them has arguably improved the end product. Field agents dig deep on a single case or target and seek evidence of wrongdoing that may support a prosecution. National Security personnel look at big picture developments and use the single case intelligence toward creation of the larger tapestry. For the most part, the Criminal Division looks to past events, while the National Security staff focuses on what may happen in the future, connecting dots and trying to make programmatic sense of information. It may make good sense to encourage greater cooperation and coordination of intelligence and law enforcement functions in response to the challenges posed by terrorism. These steps should be taken, however, without giving up the advantages of the specialization and rivalry between them.

The finger pointing at intelligence failures before September 11 is also lamentable for another reason. Hindsight visions are rarely clear before the fact. As is its nature, the intelligence "dots" that were discovered in the weeks and months before the attacks were ambiguous and imprecise. It is tempting, but far too easy now to say in retrospect, that the government could have known what was coming.

Government works best when the branches work together, and when different parts of the executive branch cooperate. The rare glimpse at the secret surveillance mechanism afforded by the release of the May 17 FISC opinion and subsequent appeal and decision in the FISCR has shown that the changing U.S. environment for counterterrorism demands that all the principal government actors must cooperate in reforming a system for such surveillance that keeps us safe and free. Unfortunately, recent developments have exposed some dissonance among those responsible for making FISA attain its aim of granting extraordinary access to intelligence information in the hands of those who would plot against the United States, while protecting the constitutional rights of all persons.