No. 02-001

IN THE UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW

IN RE [deleted]

ON APPEAL FROM THE UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT

SUPPLEMENTAL BRIEF FOR THE UNITED STATES

JOHN ASHCROFT
Attorney General

LARRY D. THOMPSON
Deputy Attorney General

THEODORE B. OLSON
Solicitor General

DAVID S. KRIS
Associate Deputy Attorney General

JAMES A. BAKER
Counsel for Intelligence Policy

JONATHAN L. MARCUS
Attorney Advisor
Department of Justice
950 Pennsylvania Avenue, NW

Washington, D.C. 20530
(202)514-2882

TABLE OF CONTENTS (U)

TABLE OF AUTHORITIES

[omitted here]

IN THE UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW

_____

No. 02-001

IN RE [deleted]

_____

ON APPEAL FROM
THE UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT

_____

SUPPLEMENTAL BRIEF FOR THE UNITED STATES

_____

INTRODUCTION

In response to the Court's invitation at the hearing in this matter on September 9, 2002, the Department of Justice submits the following supplemental brief. Part I of the brief explains the origins of the (false) dichotomy that arose between law enforcement and non-law enforcement methods of protecting against the foreign

threats to national security specified in 50 U.S.C.§ 1801(e)(1). It traces the history of Executive and Judicial Branch interpretations of FISA from 1979 to 1995.

Part II demonstrates how the USA Patriot Act's "significant purpose" and "coordination" amendments were together designed to overcome prior judicial interpretations of FISA. It argues that the "significant purpose" amendment does not affirmatively codify or inscribe into FISA the (false) dichotomy between foreign intelligence and law enforcement.

Part III responds to the Court's question concerning the continuing applicability of *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), which adopted a "primary purpose" test for electronic surveillance conducted without prior judicial authorization. It argues that *Truong* does not govern electronic surveillance conducted under FISA, and that the "significant purpose" test is constitutional.

An appendix to the brief presents a detailed comparison of FISA and Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522, particularly as applied to U.S. persons who are "agents of a foreign power" under the rubric of international terrorism, 50 U.S.C. § 1801(b)(2)(C) and (E). The appendix also discusses the constitutional significance of the differences between the two statutes as applied in such cases.

ARGUMENT

I. ORIGINS OF THE (FALSE) DICHOTOMY BETWEEN FOREIGN INTELLIGENCE AND LAW ENFORCEMENT EFFORTS TO PROTECT NATIONAL SECURITY

At the hearing on September 9, the Court asked why the government historically had not argued, and the courts generally had not held, that "foreign intelligence information" includes information sought for a prosecution designed to protect against the threats specified in 50 U.S.C. S 1801(e)(1), such as espionage and international terrorism. The discussion below reports the history of Executive and Judicial interpretations in this area, both before and after FISA.

A. Electronic Surveillance Prior to FISA.

From the beginning of the 20th Century, the United States conducted warrantless electronic surveillance for the purpose of protecting national security from foreign threats. H.R. Rep. No. 95-1283, Part I, 95th Cong., 2d Sess. 15-22 (1978) [hereinafter House Report). Although the Supreme Court never addressed the legality of such surveillance, "virtually every court that had addressed the issue had concluded that the President had the inherent power to collect foreign intelligence information, and that

such surveillances constituted an exception to the warrant requirement of the Fourth Amendment." *United States v. Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (citing cases). Four courts of appeals - the Third, Fourth, Fifth, and Ninth Circuits - upheld warrantless electronic surveillance conducted for a foreign intelligence purpose. See *ibid*. The D.C. Circuit suggested in dictum in a plurality opinion that a warrant would be required, but did not decide the issue, and no court ever held that a warrant was required. See *Zweibon v. Mitchell*, 516 F.2d 594, 633-651 (D.C. Cir. 1975).

Prior to FISA, the law did not precisely define the permissible scope of such surveillance. Courts sometimes suggested that the warrant exception depended on the existence of a foreign threat to national security, such as espionage or international terrorism, rather than an ordinary criminal threat to domestic order, such as rape or homicide. Under this approach, the government could use warrantless electronic surveillance to investigate or protect against a national security threat using any lawful means at its disposal, apparently including criminal prosecution. On other occasions, however, courts suggested that the exception also depended on the type of response or effort used to address the national security threat - i.e., that it required a traditional counterintelligence response, such as efforts to recruit a foreign spy as a double agent, rather than a law enforcement response, such as efforts to prosecute a spy for espionage. Under that approach, the government could not conduct warrantless electronic surveillance for the purpose of gathering evidence to prosecute a spy, although it could use as evidence any information that had been gathered for a non-law enforcement purpose.

In *United States v. Clay*, 480 F.2d 165 (5th Cir. 1970), the first court of appeals decision significantly addressing the issue, electronic surveillance of the defendant was initially revealed after his conviction for refusing induction into the armed forces had been affirmed on appeal. The district court concluded that the warrantless "surveillance was lawful, having been authorized by the Attorney General, for the purpose of obtaining foreign intelligence information," and the court of appeals affirmed because the surveillance was conducted "in connection with obtaining foreign intelligence information." *Id*. at 170. The court did not elaborate on the precise purpose of the surveillance, or distinguish between law enforcement and non-law enforcement efforts to protect national security. Nor did it attempt precisely to define the term "foreign intelligence information." That may be because the defendant in *Clay*was incidentally intercepted during electronic surveillance of other targets, suggesting that the purpose of the surveillance had nothing to do with his prosecution. *Ibid*. In any event, the court also found that "in no way has this wiretap prejudiced defendant, helped build a case against him, or assisted in bringing about his conviction." *Ibid.* The Fifth Circuit followed *Clay*in *United States v. Brown*, 484 F.2d 418, 426, 427(1973), upholding warrantless surveillance where it was conducted

"in connection with obtaining foreign intelligence information," the defendant was not the target, and "the information disclosed by the wiretaps had no relevancy whatever to the crime here in question, either directly or indirectly."

In *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc), the warrantless electronic surveillance was "designed to impair the escape to foreign powers of sensitive information concerning the foreign policy and military posture of the United States" - i.e., to prevent espionage. Id. at 605 n.l. The court saw "no reason to distinguish this activity from the foreign intelligence gathering activity that may be conducted through warrantless electronic surveillance, observing that "[a]s Commander-in-Chief, the President must guard the country from foreign aggression, sabotage, and espionage." Id. at 605 n.1, 608. Thus, the court recognized that protecting the United States against espionage is a "foreign intelligence purpose," and that warrantless electronic surveillance may be used in furtherance of that purpose.

The *Butenko* court did not, however, clearly resolve whether such surveillance may be conducted in support of law enforcement efforts to protect national security, such as a prosecution for espionage. The court's only extended discussion of the matter was ambiguous (494 F.2d at 606):

> Since the primary purpose of these searches is to secure foreign intelligence information, a judge, when reviewing a particular search must, above all, be assured that this was in fact its primary purpose and that the accumulation of evidence of criminal activity was incidental. If the court, for example, finds that members of a domestic political organization were the subjects of wiretaps or that the agents were looking for evidence of criminal conduct unrelated to the foreign affairs needs of a President, then he would undoubtedly hold the surveillances to be illegal and take appropriate measures.

The first underlined passage above suggests that warrantless surveillance may not be conducted for the purpose of supporting any prosecution. The second underlined passage, however, suggests that the prohibition applies only when the prosecution is "unrelated to the foreign affairs" - i.e., when it is not intended to protect national security. The court in *Butenko*did not have to resolve the issue because the defendant agreed that the surveillance was conducted "solely for the purpose of gathering foreign intelligence information," and that "he was [not] the object of surveillance because of domestic political activity or because of conduct unrelated to his own espionage concerns." Id. at 607.

Finally, in *United States v. Buck*, 548 F.2d 871 (9th Cir.1977), a firearms prosecution, the court relied on *Clay* and *Butenko* for the proposition that "[f]oreign security wiretaps are a recognized exception to the general warrant requirement." Id. at 875.

The court did not discuss the precise purpose of the surveillance, or any distinction between law enforcement and non-law enforcement efforts to protect national security. The court also noted that there was "no discernible nexus between the alleged illegal surveillance and the matters to be proved at trial." Id. at 874. Thus, no court of appeals decision issued prior to FISA squarely determined whether warrantless electronic surveillance could be used to support law enforcement efforts to protect national security - e.g., the prosecution of a spy or international terrorist.

B. Electronic Surveillance After FISA.

When Congress enacted FISA in 1978, it was aware of the decisions cited above, and of lingering questions concerning the validity and permissible scope or purpose of foreign intelligence electronic surveillance. See House Report at 19-20. In enacting FISA, with the support of the Executive Branch, Congress sought to answer those questions, setting forth in the statute "the circumstances which ultimately determine the reasonableness of a search," including "the nature, circumstances, and purpose of the search, the threat it is intended to address, and the technology involved." Id. at 20. Of particular relevance here, Congress concluded that "the purpose" of FISA surveillance must be to obtain "foreign intelligence information," 50 U.S.C. § 1804(a)(7)(B), but it defined the latter term in a way that does not discriminate between law enforcement and other methods of protecting against espionage, international terrorism, and the remaining threats specified in 50 U.S.C. § 1801(e)(1). As detailed below, neither the Executive Branch nor the courts fully implemented the original meaning of the statute.

1. The Decision in Truong.

The first significant judicial decision issued after FISA, *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), actually applied pre-FISA standards to review warrantless electronic surveillance conducted before the statute's enactment. See id. at 914 n.4, 915. The court in *Truong* upheld the use of warrantless electronic surveillance, concluding that "the needs of the executive are so compelling in the area of foreign intelligence * * * that a uniform warrant requirement would unduly frustrate the President in carrying out his foreign affairs responsibilities." Id. at 913. The court identified three reasons for that conclusion: "the need of the executive branch for flexibility, its practical experience, and its constitutional competence" as the "pre-eminent authority in foreign affairs." id. at 914.

The court in *Truong* held that "the executive branch should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons." 629 F.2d at 915. By "foreign intelligence reasons," the court meant reasons other than conducting a criminal investigation or prosecution. Thus, the court upheld

the electronic surveillance in question because its purpose "was to determine Truong's source or sources for government documents" so that the U.S. government could stanch the flow of classified information to the government of Vietnam. Id. at 916. The court held, however, that warrantless surveillance was not permitted "once surveillance becomes primarily a criminal investigation," or "when the government is primarily attempting to form the basis for a criminal prosecution." Id. at 915.[1]

> [1] The court in *Truong* did not distinguish between ordinary prosecutions (e.g., of an ordinary American citizen for homicide) and prosecutions of an agent of a foreign power to protect against espionage or terrorism. See 629 F.2d at 916. However, the court also did not explicitly reject such a distinction. On the contrary, although *Truong* involved a prosecution for espionage, the court never discussed the government's motives for the prosecution, and from all that appears the government never advanced the idea that a purpose to obtain evidence for an espionage prosecution can itself be a "foreign intelligence" purpose. Attorney General Griffin Bell, who testified at the suppression hearing in the district court, described prosecution only as an "incidental" by product of a non-criminal counterintelligence investigation: "Let me say that every one of these counterintelligence investigations involved, nearly all of them that I have seen, involves crime in an incidental way. You never know when you might turn up with something you might want to prosecute." Id. at 916 n.5.

2. The Department's Resvonse to Truong.

In the wake of *Truong*, the Department of Justice took the position that electronic surveillance under FISA required only a "significant" foreign intelligence purpose. In September 1983, the Department advised Congress that "the logic of [*Truong*] has little vitality after the enactment of" FISA. *Implementation of the Foreign Intelligence Surveillance Act*, H.R. Rep. No. 98-738, 98th Cong., 2d Sess. 14 (1984) [hereinafter House Five Year Report]. Instead, the Department argued that FISA may be used for a "significant" foreign intelligence purpose, and that such a purpose may not be undermined even if the government is contemplating a criminal prosecution (ibid.):

> even where the government may be considering prosecuting the target for criminal violations discovered during the counterintelligence investigation, the government may continue to employ FISA rather than Title III where significant foreign intelligence information is still being sought. Where no significant foreign intelligence interest remains in an investigation, FISA should no longer be used.

Similarly, in 1984, Department advised Congress that FISA should be available "so long as [the surveillance] is in furtherance of a legitimate and reasonable intelligence purpose," although it acknowledged that "[w]hether it makes any difference if criminal prosecution is contemplated when a FISA surveillance is authorized is an unresolved legal issue." *The Foreign Intelligence Surveillance Act of 1978: The First Five Years*, S.Rep. No. 98-660, 98th Cong., 2d Sess. 20, 12 (1984) [hereinafter Senate Five Year Report].

The Department's first set of FISA minimization procedures defined "foreign intelligence information" to include evidence of crimes such as espionage and international terrorism. Those procedures, which were provided to the Congressional Intelligence Committees, noted that "foreign intelligence information" may "also [be] evidence of a crime," and distinguished such information from "evidence of a crime which is not otherwise foreign intelligence information." House Five Year Report at 18. (The current procedures, which are being lodged with the Court, are similar.) This distinction, which is reflected in FISA itself, 50 U.S.C. § 1801(h), underlies the argument in our principal brief that the prosecution of a foreign spy or terrorist is a "foreign intelligence" purpose. See Gov't Br. 41-45.

The issue of whether prosecution may be a "foreign intelligence" purpose was also discussed by the Senate Intelligence Committee in a report issued in 1984 pursuant to 50 U.S.C. § 1808(b). Reviewing FISA's legislative history, the Committee stated:

> FISA does indeed contemplate the possible use in criminal proceedings of information derived from electronic surveillances. The Committee's 1978 report accompanying FISA recognized, moreover, that FISA surveillance would be * * * "part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnaping, and terrorist acts committed by or on behalf of a foreign power. Intelligence and law enforcement tend to merge in this area." The [1978] report made a particularly strong case in the counterintelligence area, noting that "foreign counterintelligence surveillance frequently seeks information needed to detect or anticipate the commission of crimes." In a later passage, however, the report states that "the primary purpose of electronic surveillance conducted pursuant to this chapter will not be the gathering of criminal evidence." Variations in judicial interpretations are thus not surprising.

Senate Five Year Report at 14 (citations omitted, emphasis added).

This statement, quoting legislative history that is also quoted in our principal brief (page 40), reflects an understanding that there is no dichotomy between intelligence

and law enforcement efforts to protect against terrorism and espionage. Other statements in the Five Year Report, however, seem to assume or adopt the dichotomy. For example, the Report notes that "[o]ne question is to what extent the FBI can use FISA surveillance to obtain both foreign intelligence information and criminal evidence for prosecution purposes." Senate Five Year Report at 14. It also states that "it is left largely to the Executive branch to determine, in individual cases, when its purpose is to obtain foreign intelligence information and when it is to prosecute criminals." Id. at 14.

As a policy matter, rather han a legal one, the Intelligence Committees opined that the Department of Justice should not use FISA primarily for law enforcement, at least against certain targets. Based on concerns that FISA's definition of "international terrorism" could reach "persons whose activities are essentially a domestic law enforcement problem," the Senate Intelligence Committee recommended that "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 surveillance will also produce some foreign intelligence information." Senate Five Year Report at 15 (emphasis added); see also id. at 20, 25. But the Committee recognized that the issue was "left largely to the Executive branch," and that FISA "leaves the FBI and Justice Department with difficult choices and responsibilities." id. at14. The House Intelligence Committee took a similar position:

> While expressing no opinion at this time as to the legal correctness of the Department's [position that FISA "may be employed, even when prosecution is contemplated, as long as significant foreign intelligence information is sought"], the Committee is of the view that, even if the Department's position is arguably supported by the relevant legislative history, the wiser course is to utilize Title III, rather than FISA, once prosecution is contemplated, unless articulable reasons of national security dictate otherwise.

House Five Year Report at 6.[2]

[2] These oversight reports, which are not directly associated with any new legislation, are subsequent history, and therefore not relevant, to the interpretation of FISA as enacted in 1978. See, e.g., *Pension Benefit Guaranty Corp. v. LTV Corp.*, 496 U.S.633, 650 (1990). As Justice Scalia put the matter in his concurring opinion in*Sullivan v. Finkelstein*, 496 U.S. 617, 632(1990), "the views of a legislator concerning a statute already enacted are entitled to no more weight than the views of a judge concerning a statute not yet passed. * * * * Arguments based on subsequent legislative history, like arguments based on antecedent futurity, should not be taken seriously, not even in a footnote."

In practice, the Department apparently allowed fairly extensive coordination between intelligence and law enforcement officials during this period. The Department's first Counsel for Intelligence Policy, Kenneth Bass, recently advised Congress that he would not "have authorized a FISA application that had its origin entirely within the law enforcement community with no prior involvement of an official in the intelligence community, had such a case ever arisen." Statement of Kenneth C. Bass, III, before the Senate Judiciary Committee, September 10, 2002, at 7 (copy of statement and transcript of hearing attached). However, Bass also stated that in his view "the purpose" to obtain foreign intelligence information would have "remained the same throughout the course of surveillance, even if there was a decision to undertake a criminal prosecution instead of a non-prosecutorial solution such as a false-flag or turning, operation." Id. at 9. Bass testified that he was "confident" that the Department'sJuly 1995 Intelligence Sharing Procedures were "not consistent with the view we held in the beginning." Id. at 6.

3. Developments From 1984 to 1993.

Between 1984 and 1993, the courts generally applied the "primary purpose" test, and either assumed or adopted the dichotomy between intelligence and law enforcement under FISA. In*United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984), the court affirmed a conviction because "the purpose of the surveillance in this case, both initially and throughout, was to secure foreign intelligence information and was not, as [the] defendants assert, directed towards criminal investigation or the institution of a criminal prosecution." In *United States v. Radia*, 827 F.2d 1458, 1464 (llth Cir. 1987), the court relied on a finding that the surveillance "did not have as its purpose the primary objective of investigating a criminal act. Rather, surveillance was sought for the valid purpose of acquiring foreign intelligence information, as defined by § 1801(e)(1)." Similarly, in *United States v. Pelton*, 835 F.2d 1067, 1075 (4thCir. 1987), the court "rejected Pelton's claim that the 1985 FISA surveillance was conducted primarily for the purpose of his criminal prosecution, and not primarily 'for the purpose of obtaining foreign intelligence information' as required by" FISA. And in *United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1992), the court relied on its conclusion that the "primary purpose" of the surveillance, "from the first authorization in July 1988, to July 1989, when appellants were arrested, was to obtain foreign intelligence information, not to collect evidence for any criminal prosecution of appellants."

Coordination between intelligence and law enforcement officials continued during this period, though perhaps not to the extent originally permitted. From 1984 to 1993, while Mary Lawton was Counsel for Intelligence Policy, the Criminal Division was regularly briefed by the FBI about ongoing intelligence investigations concerning espionage, but prosecutors "knew we were not to 'direct' the [intelligence]

investigation or to suggest the use of FISA for criminal investigative purposes." *IV Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation*, Chapter 20, at 711 (May 2000) [hereinafter AGRT Report]. The briefings allowed the Criminal Division to assert that a case should be prosecuted. The FBI and the Criminal Division were permitted to consult without informing OIPR, and without OIPR being present. id. at 712.

4. The July 1995 Procedures.

In 1993 and early 1994, during the investigation of Aldrich Ames, coordination between intelligence and law enforcement officials apparently again became quite robust. As explained in the AGRT Report, the Counsel for Intelligence Policy at that time, Richard Scruggs, "went to the Attorney General and 'ginned her up' about contacts that the FBI had been having with prosecutors" in the Ames case. AGRT Report at 713. Scruggs "raised concerns with the Attorney General that the FISA statute had been violated by these contacts and that her certifications [i.e., her approval of FISA applications for filing with the FISC] had been inaccurate. Scruggs believed that the relationship between the FBI and [the Criminal Division's Internal Security Section] during the Ames investigation could be used by defense counsel to cast doubt upon the 'primary purpose' of the FISA surveillance and thereby jeopardize the prosecution." Ibid. Thereafter, according to the AGRT Report, the "'backdoor' channel between the FBI and [the Criminal Division] was closed." Id. at 714.

The July 1995 Intelligence Sharing Procedures had their origins in a June 1994 memorandum written by Allan Kornblum, then the Deputy Counsel in OIPR. AGRT Report at 714 & n.949.[3] This proposal "touched off considerable controversy and led to a series of meetings among the principals in the Criminal Division, OIPR, the FBI * * * and [a component of the Office of the Deputy Attorney General]." Id. at 715. On February 14, 1995, as part of the deliberative process, the Department's Office of Legal Counsel (OLC) prepared a memorandum on the "primary purpose" standard. Id. at 720. In light of *Truong, Duggan, Radia, Pelton*, and *Johnson*, the OLC memorandum predicted that "courts are more likely to adopt the 'primary purpose' test than any less stringent formulation." OLC memo at 1. The memorandum also recognized the dichotomy between intelligence and law enforcement that had been assumed in those cases, noting that "the greater the involvement of prosecutors in the planning and execution of FISA searches, the greater is the chance that the government could not assert in good faith that the 'primary purpose' was the collection of foreign intelligence." Ibid.; see id. at 2, 5 & n.7. As discussed in the AGRT report, the OLC memorandum influenced the standards adopted in the July 1995 Procedures. AGRT Report 720.

[3] The original proposal was to modify the Attorney General's Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations. AGRT Report 714. Those classified Guidelines govern the conduct of investigations generally, and do not pertain exclusively to the use of FISA. Those Guidelines are to be distinguished from the FBI's classified Standard Minimization Procedures, which deal exclusively with minimization under FISA, and from the unclassified July 1995 and March 2002 Intelligence Sharing Procedures, which (in the Department's view, at least) deal not with minimization but with coordination between intelligence and law enforcement officials. With this brief, we are also lodging with the Court copies of the current versions of the Attorney General's classified Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations, and the classified Standard minimization Procedures.

The July 1995 Procedures limited the nature and extent of consultations between the Criminal Division and the FBI, and also required careful documentation and reporting to the FISC of such consultations. Where FISA was being used in a foreign intelligence (FI) or foreign counterintelligence (FCI) investigation, the Criminal Division was allowed to give "guidance to the FBI aimed at preserving the option of a criminal prosecution," but was not expressly authorized to give advice aimed at "enhancing" the possibility of a criminal prosecution. The July 1995 Procedures cautioned the Criminal Division and the FBI to "ensure" that any advice given did "not inadvertently result in either the fact or the appearance of the Criminal Division's directing or controlling the FI or FCI investigation toward law enforcement objectives." July 1995 Procedures, Part A, P. 6. The procedures also required the FBI to maintain "a log of all contacts with the Criminal Division," and required all FISA renewal applications to "apprise the FISC of the existence of, and basis for, any contacts among the FBI, the Criminal Division, and a U.S. Attorney's Office, in order to keep the FISC informed of the criminal justice aspects of the ongoing investigation." Id. Part A, PP 4, 7.

With some notable exceptions, the July 1995 Procedures significantly limited consultations between law enforcement and intelligence officers where the Department wanted to preserve its ability to use FISA. Amendments to the procedures adopted in August 2001 ensured that the Criminal Division was entitled to all relevant information obtained from FISA searches or surveillance, but contacts between the FBI and the Division were required to be coordinated with OIPR. Moreover, although the July 1995 Procedures permitted advice designed to "preserve" the possibility of a prosecution, the procedures were understood to ban advice designed to "enhance" the possibility of a prosecution, and the line between "preserving" and "enhancing" advice is so murky that advice-giving was substantially curtailed. See AGRT Report at 721-

734; General Accounting Office, *FBI Intelligence Investigations: Coordination within Justice on Counterintelligence Criminal Matters is Limited* (July 2001) (GAO-01-780) (hereinafter GAO Report).

II. THE USA PATRIOT ACT DOES NOT CODIFY THE (FALSE) DICHOTOMY BETWEEN INTELLIGENCE AND LAW ENFORCEMENT EFFORTS TO PROTECT NATIONAL SECURITY

It is against the foregoing historical background, particularly as recounted in the AGRT and GAO Reports, that the USA Patriot Act was passed by Congress and should be interpreted by this Court. Both the "coordination" amendment (50 U.S.C. § 1806(k)) and the "significant purpose" amendment (50 U.S.C. § 1804(a)(7)(B)) were designed to facilitate greater coordination between intelligence and law enforcement officials, and to overturn prior standards restricting that coordination. As explained in the government's principal brief, however, each amendment attacks the problem differently. The coordination amendment rejects the dichotomy between law enforcement and non-law enforcement methods, and reaffirms the original statutory definition of "foreign intelligence information" to include information sought for use in a law enforcement effort to protect against espionage or international terrorism (e.g., the prosecution of Robert Hanssen or Ahmed Ressam). See Gov't Br.30-41. The significant purpose amendment, by contrast, does not address the scope or definition of foreign intelligence information or a foreign intelligence purpose; it merely reduces the degree of foreign intelligence purpose required to use the statute, and makes clear that the inquiry into the government's purpose is not comparative. See id. at 49-56.

A. The Patriot Act Amendments Were Designed to Override Prior Adoptions of the (False) Dichotomy.

The significant purpose and coordination amendments together restore FISA to its original meaning and function. Especially given the context surrounding their enactment, the two amendments represent a sensible response to the situation Congress confronted in September 2001: A statute whose plain language rejects the dichotomy between foreign intelligence and law enforcement, but a FISC (and other courts) that had ignored that language and adopted the dichotomy. Faced with that gap between FISA's original meaning and its judicial interpretation, Congress was not required to adopt one approach or the other - i.e., it was not required to choose between (1) abandoning its original intent in enacting FISA, or (2) proceeding as if the intervening cases were never decided. Instead, Congress wisely pursued both approaches to the problem, reaffirming the original intent of the statute but also dealing pragmatically with the reality that the courts had misinterpreted it.

By enacting both amendments Congress doubled the chances that its intent would be carried out. See 50 U.S.C. §§ 1804(a)(7)(B), 1806(k). Thus, the coordination amendment was designed to force the courts to abandon the false dichotomy between foreign intelligence and law enforcement. But even if that effort failed, and courts maintained the false dichotomy, the significant purpose amendment would still grant the government substantial relief by increasing the allowable amount of law enforcement purpose. Moreover, enacting two amendments also provided insurance against any constitutional problems that courts might find with either amendment. In the face of a national crisis of the first order, and an extremely compressed legislative schedule, Congress chose an eminently reasonable approach.

Although the significant purpose amendment does not challenge the dichotomy between foreign intelligence and law enforcement, neither does it affirmatively adopt or codify that dichotomy. To be sure, while "CoDngress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statutewithout change," *Lorillard v. Pons*, 434 U.S. 575, 580 (1978) (emphasis added), such presumptions cannot hold where Congress amends a statute specifically to deal with prior administrative or judicial interpretations. This conclusion is especially strong where, as here, the agency and judicial interpretations are fundamentally at odds with the plain language of the original statute. See, e.g., *Brown v. Gardner*, 513 U.S. 115, 121 (1994); *Demarest v. Manspeaker*, 498 U.S. 184 (1991). As the Supreme Court has long recognized, "[w]here the law is plain the subsequent reenactment of a statute does not constitute adoption of its administrative construction." *Biddle v. Commissioner*, 302U.S. 573, 582 (1938).

Nor does the fact that Congress chose not to amend the definition of "foreign intelligence information" signify acquiescence in prior interpretations adopting the false dichotomy between intelligence and law enforcement. Congress did not rely on the Administration's or the courts' prior position to pass the Patriot Act, a crucial consideration for acquiescence. See *F.D.A. v. Brown & Williamson Tobacco Corp*., 529 U.S. 120, 156 (2000). On the contrary, Congress sought to help the Administration overcome both the crabbed construction of "foreign intelligence information" and the wall of separation between intelligence and law enforcement, a fact that the President clearly understood when he signed the legislation:

> For example, this legislation gives law enforcement officials better tools to put an end to financial counterfeiting, smuggling and money-laundering. Secondly, it gives intelligence operations and criminal operations the chance to operate not on separate tracks, but to share vital information so necessary to disrupt a terrorist attack before it occurs.

> As of today, we're changing the laws governing information-sharing. And as importantly, we're changing the culture of our various agencies that fight terrorism. Countering and investigating terrorist activity is the number one priority for both law enforcement and intelligence agencies.

President's Remarks on Signing the USA Patriot Act of 2001, 37 Weekly Comp. Pres. Doc. 1550 (Oct. 29, 2001). As this statement recognizes, both intelligence and law enforcement can (and must) work together to protect against international terrorism. It follows *a fortiori*that this is not a case with "overwhelming evidence of acquiescence," as thd Supreme Court generally requires. See *Solid Waste Agency of N. Cook County v. United States Army Corps of Eng'rs*, 531 U.S. 159, 169-170 & n.5 (2001). While the "significant purpose" amendment recognizes the existence of the dichotomy between foreign intelligence and law enforcement, it cannot be said to recognize (or approve) its legitimacy.

Indeed, it would be particularly anomalous to read the significant purpose amendment as an affirmative enactment of the false dichotomy. As noted above, Congress did not adopt the significant purpose amendment because it was in agreement with prior judicial decisions adopting the false dichotomy. On the contrary, the amendment represents a cleardisagreement with the result reached in those decisions. Thus, it is only by negative implication from Congress, rejection of the judicial primary purpose standard that it is possible to read the amendment as an affirmation of the judicially-adopted dichotomy between law enforcement and non-law enforcement efforts to protect national security.

Such a reading of the USA Patriot Act would amount to an inversion of Congress' fundamental intent in passing the law. It is one thing to conclude that reenactment of a statute without addressing prior judicial constructions amounts to a tacit adoption of those constructions - i.e., that Congressional "silence is acceptance." It would be quite another thing, however, to conclude that amending a statute to change prior judicial constructions amounts to adoption of other aspects of those constructions - i.e., that "rejection is acceptance." While the significant purpose amendment did not specifically reject the false dichotomy, it also did not ratify or adopt that dichotomy. The most that can be said is that the amendment is silent or agnostic on the issue.

Given that silence, the plain language of the 1978 version of FISA continues to govern. See*United States v. Vonn*, 122 S.Ct. 1013, 1050 (2002) (adoption of harmless error standard for guilty pleas in Fed. R. Crim. P. 11(h) does not implicitly repeal plain error standard in Fed. R. Crim. P. 52(b)). Indeed, the significant purpose amendment cannot implicitly repeal the definition of "foreign intelligece information" because Congress simultaneously and expressly reaffirmed that definition (and repeated its operative language verbatim) by enacting the coordination amendment.

Any attempt to read the "significant purpose" amendment as an implicit repeal of FISA's original meaning therefore runs headlong into the unambiguous intent of Congress to perpetuate that meaning through the coordination amendment. As Senator Leahy stated in explaining the coordination amendment, "[p]rotection against these foreign-based threats by any lawful means is within the scope of the definition of foreign intelligence information,' and the use of FISA to gather evidence for the enforcement of these laws was contemplated in the enactment of FISA." 147 Cong. Rec. S10990-02, at S11004 (October 25, 2001). In short, as the D.C. Circuit has observed in a similar context:

> Were we to infer congressional approval of [the Department of] Interior's rules because it did not amend the statute to explicitly repudiate them, we would in effect be insisting that a Congress legislatively reiterate an already clear statutory command in order to fend off an impermissible interpretation. As we all know, many statutes are on the books for which no congressional majority could presently be garnered either to reenact or to repeal, yet those acts continue as valid law; indeed, a canon of equal worth with the acquiescence-by-reenactment rule is the one disfavoring repeal by implication. We conclude that the acquiescence-by-reenactment rule is not applicable to a situation where the regulations violate the original statutory language and where Congress' decision not to amend the relevant statutory provisions evidently stems from a belief that the provisions have been clear all along.

State of Ohio v. Department of the Interior, 880 F.2d 432, 458-459 (D.C. Cir. 1989) (emphasis in original).

B. Each of the Patriot Act Amendments Has Independent Meaning When Read Together.

Each of the Patriot Act amendments has an effect when read as the government proposes. The coordination amendment, of course, reaffirms that information sought for certain prosecutions is "foreign intelligence information." See Gov't Br. 30 49. It therefore allows unfettered coordination between intelligence and law enforcement officials in furtherance of efforts to protect against espionage and international terrorism. It also ensures that such coordination cannot preclude a certification or finding of the required significant foreign intelligence purpose.

For its part, the significant purpose amendment makes clear that judicial review of the government's purpose is not comparative. See Gov't Br. 51-54. Thus, it reduces the need for judicial inquiry into any purpose other than a purpose to obtain "foreign intelligence information." In theory, of course, many such (non-foreign intelligence) purposes are possible -- e.g., surveillance for the purpose of domestic political

harassment, or even for sheer voyeurism. In practice, however, the only "other" purpose likely to arise is an "ordinary" law enforcement purpose- i.e., a purpose to obtain evidence for a prosecution that is not intended to protect against the foreign threats to national security specified in 50 U.S.C. §§ 1801(e)(1) and 1806(k)(1).

Obviously, some federal prosecutions are intended to protect against those threats, and some are not. In many cases, the purpose of the prosecution will be evident from the nature of the defendant and the charges. Thus, where an agent of a foreign power is prosecuted for espionage or terrorism, or offenses directly related to espionage or terrorism (e.g., providing material support to terrorists, 18 U.S.C. § 2339A), the inference is all but unavoidable that the prosecution represents a "foreign intelligence purpose under FISA. Correspondingly, where the prosecution concerns someone who is not an agent of a foreign power for an offense that is no related to those threats - e.g., the prosecution of Bonnie and Clyde for bank robbery - the opposite is true.

Between those extremes, the purpose of the prosecution may vary with the particular case. For example, where the government has inescapable evidence that a FISA target is engaged in espionage, but the evidence cannot be authenticated or introduced at a public trial without compromising a valuable intelligence source or method, there may be no alternative but to prosecute the spy for another offense, such as mail fraud. In such a case, the mail fraud prosecution would be a "foreign intelligence" purpose under FISA because it would be intended to protect against espionage. Mail fraud prosecutions conducted to deter financial crime or to reassure investors concerning the integrity of the financial system, however would not constitute a "foreign intelligence" purpose, even if the defendant also happened to be an agent of a foreign power.

Under the significant purpose amendment, where the Director of the FBI certifies the government's foreign intelligence purpose, courts generally should not require the government to provide detailed information about the conduct of its investigation. The significant purpose amendment thus recognizes the Executive Branch's expertise in identifying the information needed to protect national security from foreign threats, and the most appropriate ways of using that information. In that respect, it too is a reaffirmation of Congress' original intent.

FISA was always intended to require deference to the Executive's expertise. As enacted in 1978, FISA did not contemplate that "judges will somehow become involved * * * in making foreign policy [or] foreign intelligence policy," or that they would "make substantive judgments as to the propriety of or need for a particular surveillance." House Report at 25. Despite this original intent, however, the AGRT and GAO reports show that in the intervening years the FISC and other courts went too far in second-guessing the government's judgments, and in regulating its investigations, particularly in the area where intelligence and law enforcement

interests overlap, and where the fluid nature of investigations calls for the utmost in Executive Branch authority. The significant purpose amendment responds to these judicial excesses.[4]

> [4] The USA Patriot Act was not the first time that the possibility of excessive judicial interference with the President's authority over national security matters had been raised. That issue was of concern even when FISA was first enacted. As one witness testified in 1978,
>
> > the judiciary is neither theoretically nor actually more neutral than the executive, or, for that matter, the Congress, in reaching answers to the difficult questions which national security electronic surveillance presents. It can as easily be argued that the judiciary will overweigh the interests of individual privacy claims because it is, after all, the protection of those claims on which judicial authorityis based * * * And since judges are not politically responsible, there is no self-correcting mechanism to remedy their abuses of power.
>
> *Foreign intelligence Electronic Surveillance: Hearings on H.R.5794, 9745, 7308, and 5632 Before the Subcomm. On Legislation of the Permanent Select Committee on Intelligence*, 95th Cong. 2d Sess. 22l (1978) (statement of Laurence Silberman).

In short, the significant purpose amendment does not incorporate the false dichotomy between intelligence and law enforcement methods of protecting against foreign spies and terrorists. The amendment does not, even implicitly, adopt that dichotomy. Statutory reenactments do not incorporate intervening case law where, as here, the cases conflict with the plain language of the original statute. Still less would it be appropriate to find such incorporation in an amendment designed to overrule the case law, albeit on other grounds, especially where a companion amendment repeats verbatim and clearly reaffirms the original statutory language. Congress had ample reason to enact both the significant purpose and coordination amendments, and each amendment may be read to serve an independent purpose and perform an independent function.

C. The Two Patriot Act Amondments Eliminate the Wall Restricting Coordination Between Intelligence and Law Enforcement Personnel

At a minimum, even if this Court rejects the foregoing argument, the USA Patriot Act nonetheless clearly changes prior practice in several important respects. First, it eliminates the "primary purpose" standard. Indeed, the "significant purpose" amendment makes clear thatlaw enforcement may be the primary purpose behind a FISA surveillance. As explained in our principal brief (pages 51-52), that is unavoidably the case in light of the plain meaning of the word "significant." The

Patriot Act's legislative history supports that view. Members of Congress who voted for and against the USA Patriot Act understood that the "significant purpose" amendment would have that effect. For example, Senator Feingold made the following statement concerning the amendment:

> The bill changes [the "primary purpose"] requirement. The Government now will only have to show that intelligence is a "significant purpose" of the investigation. So even if the primary purpose is a criminal investigation, the heightened protections of the fourth amendment will not apply.

147 Cong. Rec. S11021 (Oct. 25, 2001). To the same effect is Senator Wellstone's statement:

> The bill broadens the Foreign Intelligence Surveillance Act, FISA, by extending FISA surveillance authority to criminal investigations, even when the primary purpose is not intelligence gathering.

147 Cong. Rec. S11025 (Oct. 25, 2001).

Perhaps most directly on point is the following colloquy between Senators Leahy and Cantwell concerning the "significant purpose" amendment:

> [Senator Cantwell:] Although the language has been improved from the administration's original proposal and now would require that 'a significant,' rather than simply 'a' purpose for the wiretap must be the gathering of foreign intelligence, the possibility remains that the primary purpose of the wiretap would be a criminal investigation without the safeguards of the title III wiretap law and the protections under the fourth amendment that those fulfill. I would like to ask the Chairman of the Judiciary Committee whether he interprets this language in this same way.
>
> [Senator Leahy:] Yes, the Senator from Washington is correct. While improved, the USA Act would make it easier for the FBI to use a FISA wiretap to obtain information where the Government's most important motivation for the wiretap is for use in a criminal prosecution.

147 Cong. Rec. S10593 (Oct. 11, 2001).

Other historical evidence also supports the conclusion. A letter sent to Congress from the Department of Justice in support of the significant purpose amendment stated that the amendment would recognize that "the courts should not deny [the President] the authority to conduct intelligence searches even when the national security purpose is secondary to criminal prosecution." App. 1:3 (attachment) at page 13. Indeed, even

contemporaneous media reports evinced an understanding of the meaning of the "significant purpose" amendment. See Congressional Quarterly, House Action Reports, Fact Sheet No. 107-33 (Oct. 9, 2001), at page 3 ("Under the measure, for example, law enforcement could carry out a FISA operation even if the primary purpose was a criminal investigation."); see also Congressional Quarterly, House Action Reports, Legislative Week (Oct. 23, 2001), at page3; Congressional Quarterly, House Action Reports, Legislative Week (Oct. 8, 2001), at page 13.

Accordingly, the significant purpose amendment, standing alone, substantially corrects the prior constriction of the range of permissible uses of FISA. Indeed, relaxing the purpose standard has a similar effect as restoring the original meaning of "foreign intelligence information." Consider a hypothetical surveillance designed primarily to gather evidence to convict a target of espionage, and secondarily (but significantly) to support non-law enforcement efforts to neutralize the spy. Under the original definition of "foreign intelligence information," which rejects the dichotomy between intelligence and law enforcement, the sole purpose of this surveillance would be to obtain foreign intelligence information. However, even if the significant purpose amendment were thought to ratify the dichotomy, it would still permit this surveillance, because a significant purpose of the surveillance is non-law enforcement. As noted in our principal brief (pages 55-56), even where the governmont's law enforcement purpose is at its zenith, there will always (or almost always) also exist a significant non-law enforcement purpose for FISA surveillance.

Accordingly, the significant purpose amendment in large measure dismantles the wall of separation between intelligence and law enforcement. But Congress did not stop there. Instead, it spoke directly to that issue, expressly authorizing intelligence agents who are conducting FISA searches or surveillance to "consult" and "coordinate" with law enforcement officers to protect against foreign threats to national security. 50 U.S.C. §§ 1806(k), 1825(k). Thus, not only did Congress provide that FISA may be used primarily for a law enforcement purpose, it also encouraged coordination between intelligence and law enforcement personnel, providing that such coordination cannot undermine the required "significant" foreign intelligence purpose. Indeed, Congress also spoke directly to the Judicial Branch, instructing the FISC that such coordination "shall not preclude * * * the entry of an order" authorizing a search or surveillance. In other words, Congress directly and unambiguously tore down the wall.

In light of Congress' intent to eliminate the wall at the center of the false dichotomy between intelligence and law enforcement purposes, it would be counterintuitive to interpret those same amendments as reaffirming the wall. Finding that Congress adopted a judicial misinterpretation *sub silentio* is a troublesome enterprise even when there is extrinsic evidence that Congress intended to affirm the judicial decisions, but

when the entire thrust of congressional action is to remove judicial impediments to an effective response to terrorist threats, it makes no sense to read those amendments as reaffirming the theoretical basis of the precise judicial decisions that the amendments attempted to overturn as a practical matter.

III. FISA MAY BE USED WHERE A "SIGNIFICANT PURPOSE" OF THE SURVEILLANCE IS TO OBTAIN FOREIGN INTELLIGENCE INFORMATION

The government's principal brief on appeal defended the constitutionality of the Patriot Act's "coordination" amendment by arguing that the Fourth Amendment does not discriminate between law enforcement efforts and other efforts to protect against the foreign threats specified in 50 U.S.C. §§ 1801(e)(1)and 1806(k)(1). The brief maintained that it is the nature of the threat - e.g., espionage or international terrorism - rather than the nature of the response that dictates the constitutional analysis. See Gov't Br. 67-74. The brief also argued that the "significant purpose" amendment is constitutional by referring to (and submitting) a letter sent to Congress in support of the amendment during the debates over the Patriot Act. Id. at 74-77.

At the hearing on September 9, this Court asked for additional briefing on whether the "primary purpose" standard is constitutionally required for FISA surveillance. In particular, the Court inquired whether the Fourth Circuit's decision in *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), governs here, and whether FISA establishes a "warrant" procedure within the meaning of the Fourth Amendment. Although the law is not entirely settled, there is support for the proposition that a FISA order is a Fourth Amendment "warrant" in the technical sense, because it is a judicial order authorizing a search based on a finding of probable cause. Whether or not such an order is a "warrant," however, it is one of many procedures that makes FISA surveillance more reasonable than unilateral Executive Branch surveillance, and therefore an important reason that the "significant purpose" standard is constitutional.

A. The President Has Inherent Authority to Conduct Warrantless Electronic Surveillance to Protect National Security from Foreign Threats.

In considering the constitutionality of the amended FISA, it is important to understand that FISA is not required by the Constitution. Rather, the Constitution vests in the President inherent authority to conduct warrantless intelligence surveillance (electronic or otherwise) of foreign powers or their agents, and Congress cannot by statute extinguish that constitutional authority. Both before and after the enactment of FISA, courts have recognized the President's inherent authority to conduct foreign intelligence surveillance. See, e.g., *Butenko*, 494 F.2d at 608 (grounding exception to warrant requirement in the President's Commander-in-chief and foreign-affairs

powers; noting that the country's self-defense needs weigh on the side of reasonableness); *Truong*, 629 F.2d at 914 (citing the President's foreign affairs power as justifying an exception to the warrant requirement); cf. *United States v. United States District Court (Keith)*, 407 U.S. 297, 308 (1972)(reserving the question whether the President's foreign-affairs powers justify exception from warrant requirement). In general, these courts have arrived at the "primary purpose" test as a result of balancing the President's inherent authority against the privacy interests that are affected by warrantless searches. See, e.g., *Truong*, 629 F.2d at 913-915.

Given the enormous - and unique - importance of the President's constitutional obligation to protect national security from foreign threats, there is a strong argument that the "primary purpose" test is too strict even for electronic surveillance conducted without prior judicial approval. The government in *Truong* argued that such surveillance is constitutional whenever there is "any degree" of foreign intelligence purpose, while the defendants supported a "sole" purpose standard. 629 F.2d at 915-916. The court of appeals adopted a compromise, settling on the "primary purpose" test, and explaining that "[w]e think that the unique role of the executive in foreign affairs and the separation of powers will not permit this court to allow the executive less on the facts of this case, but we also are convinced that the Fourth Amendment will not permit us to grant the executive branch more." Id. at 916. Nonetheless, the court did not expressly consider or reject the "significant" purpose standard as an alternative to the "primary" purpose standard.

The factors favoring warrantless foreign intelligence searches have become substantially more compelling in the wake of the attacks of September 11. The government's interest has shifted to defense of the Nation from violent attack. "It is more obvious and unarguable that no governmental interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981) (citation and quotations omitted). While the magnitude of the current threat alone justifies expanding the warrant exception to searches with a significant foreign intelligence purpose, the nature of the threat is also an important consideration. Combating international terrorism is inescapably both a foreign affairs and a law enforcement function. In this context, separation-of-powers concerns require a relaxation of that standard.

B. The "Significant Purpose" Test for FISA Surveillance Satisfies the Constitution.

This Court need not decide whether the "primary purpose" test would govern unilateral Executive Branch surveillance conducted today, because the surveillance at issue here is governed by FISA's extensive procedural protections. As mentioned above, FISA orders are issued pursuant to individualized suspicion by an Article III

judge. The statute requires certifications from high-ranking Executive Branch officials. It provides for intricate minimization procedures and extensive congressional oversight. And it requires a finding of probable cause - albeit not always the same probable cause that is required in ordinary criminal cases.

To the extent that FISA does not require ordinary probable cause, there is support for the proposition that a FISA order is a "warrant" in the constitutional sense. See, e.g., *Griffin v. Wisconsin*, 483 U.S. 868, 877 n.4 (1987); *Camara v. Municipal Court*, 387 U.S. 523, 534 (1967); *Keith*, 407 U.S. at 322-23. The courts of appeals have referred to FISA orders as "warrants" in the constitutional sense. See, e.g., *Pelton*, 835 F.2d at 1075; *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987)(Kennedy, J.). The Court in *Keith* did not suggest that electronic surveillance conducted under standards different from those in Title III would fall outside the Warrant Clause. See 407 U.S. at 323.

But even if FISA orders are not warrants in the constitutional sense, the pivotal question for Fourth Amendment purposes is whether FISA-authorized surveillance is reasonable. The Supreme Court has upheld the use of administrative search warrants issued without a traditional showing of probable cause. In *Camara*, for example, the Court held that routine inspections for violations of a city's housing code required a "warrant procedure." 387 U.S. at 534. However, the Court went on to hold, in this "administrative warrant" context, that the probable cause standard should be "reasonableness." See id. at 537, 539. The Court specifically rejected the contention that such "warrants should issue only when the inspector possesses probable cause to believe that a particular dwelling" was in violation of the code, let alone when there is probable cause of a crime. Id.at 534; cf. *Keith*, 407 U.S. at 322-23 (noting that a lower probable cause standard may satisfy the Fourth Amendment in domestic security cases).

Indeed, the Supreme Court has also upheld warrantless and suspicionless searches undertaken for reasons other than ordinary, general law enforcement. See, e.g., *Vernonia*, 515 U.S.at 652-653. The Court has recognized that special law enforcement needs - in particular, needs related to foreign affairs and national security - can justify such warrantless and suspicionless searches. See, e.g., U*nited States v. Martinez-Fuerte*, 428 U.S. 543, 552 (1976) (upholding permanent immigration checkpoints, in part, due to the "formidable law enforcement problems" inherent in stemming the flow of illegal immigration); *City of Indianapolis v. Edmond*, 531 U.S. 32, 38 (2000)(characterizing *Martinez-Fuerte* as reflecting the "longstanding concern for the protection of the integrity of the border"); see also*Illinois v. McArthur*, 531 U6S. 326, 330 (2001) ("When faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that

certain general, or individual, circumstances may render a warrantless search or seizure reasonable" (emphasis added)(citations omitted)).

Whether or not FISA establishes a "warrant" procedure, it clearly imposes procedural protections far beyond those associated with unilateral Executive Branch surveillance of the sort at issue in *Truong*. Thus, FISA surveillance is distinguishable from unilateral surveillance, if not under the Warrant Clause of the Fourth Amendment, then at least under the Reasonableness Clause. As the Supreme Court recognized in the *Keith* case, "security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime,'" and may therefore support standards "which differ from those already prescribed for specified crimes in Title III." 407 U.S. at 322-323. These different standards, the Court explained in *Keith*, are "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." Id. at 323. At issue in *Keith* was protection against domestic threats to national security. This case, of course, involves protection of the country from foreign threats, and therefore implicates even more important government interests, and the core of the President's Article II powers. See *Haig v. Agee*, 53 U.S. 280, 307 (1981) ("no government interest is more compelling than the security of the Nation").

C. The FISC's Decision Improperly Micromanages the Executive Branch in Violation of Articles II and III of the Constitution.

Apart from any constitutional defense of the Patriot Act as interpreted by the government, there are significant constitutional questions raised by the FISC's May 17 order - particularly the "chaperone" requirement and the reporting requirements of its new Rule 11. No Supreme Court opinion has ever recognized the authority of a federal court to impose such structural requirements on the Executive, let alone with respect to such core executive functions. The reasons for this are clear: Article III simply does not grant federal courts any power to order the internal workings of the Executive Branch, particularly in the area of foreign intelligence. But even if federal courts had some power to micromanage the Executive Branch, separation of powers prohibits the use of that power to the extent it interferes with core functions of the Executive.

First, nothing in the text of Article III even hints that federal courts have authority to micromanage the Executive Branch. By its plain terms, Article III makes clear that the judicial power is limited to cases and controversies. See U.S.Const. Art. III, 5 2. This limitation "defines the role of the judiciary in a tripartite allocation of power to assure that the federal courts will not intrude into areas committed to other branches of government." *United States Parole Comm'n v. Geraghty*, 445 U.S. 388, 396 (1980) (internal quotation and citation omitted). Federal courts must "carefully abstain from

exercising any power that is not strictly judicial in its character, and which is not clearly confided in [them] by the Constitution."*Muskrat v. Brown*, 219 U.S. 346, 355 (1911)(internal quotation omitted). Here, the FISC went beyond the mere decision of an Article III case or controversy by attempting to impose rules for the operation of the Executive Branch and structure the functions of different units with the Executive Branch.

Even if Article III provided some justification for the FISC's actions, separation of powers required the FISC not to interfere with the Executive's core functions. The Supreme Court has long recognized that the core powers conferred on each branch cannot be shared with the other branches. See, e.g., *United States v. Nixon*, 418 U.S. 683, 704 (1974). Even in*Morrison v. Olson*, 487 U.S. 654, 695 (1988), in which the Court upheld the role of the Special Division Court to appoint independent counsels under the Ethics in Government Act, the Court explained that the Act did not "work[] any judicial usurpation of properly executive functions." The powers conferred upon the Special Division were "not supervisory or administrative, nor [were] they functions that the Constitution requires be performed within the Executive Branch." Ibid.[5] it seems clear that if a federal court had assumed supervisory or administrative functions over Executive Branch officers, the Supreme Court would have found it to be a violation of the separation of powers.

> [5] Additionally, the Court construed the Special Division's power to terminate the office of the independent counsel as ministerial, in order to avoid the constitutional problem of usurping Executive authority. See 487 U.S. at 682-83.

Concern about the appropriate role of the Article III judiciary is especially pronounced where, as here, the case involves the functions of the Executive Branch in the area of national security. The Supreme Court has explained that "no government interest is more compelling than the security of the Nation." *Haig v. Agee*, 453 U.S. 280, 307 (1981). The text, structure, and history of the Constitution demonstrate that the primary responsibility to protect this interest is vested in the President. Article II, section 2 states that he "shall be Commander in Chief of the Army and Navy of the United States." The Constitution also vests in the President all of the executive power and imposes on him a duty to execute the laws. These powers give the President broad constitutional authority to respond to threats to the national security. See, e.g., *Johnson v. Eisentrager*, 339 U.S. 763, 789 (1950); *Loving v. United States*, 517 U.S. 748, 776 (1996) (Scalia, J., concurring) (noting that the "inherent powers" of the Commander in Chief "are clearly extensive"). Further, as the courts have repeatedly recognized, the President possesses exclusive power over the conduct of foreign affairs. See, e.g., *United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 320 (1936); see also*Department ofthe Navy v. Egan*, 484 U.S. 518, 529 (1988). The

conduct of foreign counterintelligence investigations is a necessary correlate to these executive powers.[6] In order to successfully defend the Nation from threats to its security, the President must have the ability to gather and disseminate foreign intelligence information that will allow him and his assistants to develop and execute the most appropriate policies. This is an area where Article III intervention is particularly unsuited, in light of the structural advantages of the Executive to act with speed, secrecy, and unity of energy, see, e.g., *The Federalist* No. 70, at 424 (Alexander Hamilton) (Clinton Rossiter ed., 1961) ("Decision, activity, secrecy, and dispatch will generally characterize the proceedings of one man in a much more eminent degree than the proceedings of any greater number"); see also *The Federalist* No. 74 (Alexander Hamilton), and the relative incompetence of the federal judiciary in such matters, see, e.g.,*Curtiss-Wright Export Corp.*, 299 U.S. at 319 ("In this vast external realm [of federal power over foreign affairs], with its important, complicated, delicate and manifold problems, the President alone has the power to speak or listen as a representative of the nation"); id. at 320 (describing the President "as the sole organ of the federal government in the field of international relations").

> [6] Indeed, as discussed above, Article II of the Constitution grants the President authority to conduct warrantless foreign intelligence surveillance when he deems it necessary to protect the Nation against foreign attack.

Prior to the USA Patriot Act, the judicial "primary purpose" standard (and the Department's internal procedures to ensure compliance with that standard) hampered the President's ability to discharge his core national security and foreign relations functions. As a result, the Department revised its procedures, pursuant to the Executive Branch's constitutionally designated powers and an explicit act of Coogress (the USA Patriot Act). The FISC, rendering its own policy judgments on how foreign counterintelligence investigations should be conducted, rejected in part and rewrote in part the Department's procedures.

To be sure, the FISC has an obligation to uphold the Constituition and, in particular, the Fourth Amendment. If the FISC determines that a particular surveillance, if authorized, would violate FISA or the Fourth Amendment, it should deny the application. The order issued by the FISC in this case, however, wholly exceeded that court's authority because it directly exercised the Executive Branch's core national security and foreign policy functions. Regardless of Article III, the FISC acted impermissibly by exercising and undermining these uniquely Executive powers.

D. The Doctrine of Constitutional Avoidance Supports the Government's Interpretation of FISA.

In light of the foregoing, the doctrine of constitutional doubt supports, and certainly does not undermine, the government's interpretation of the Patriot Act. See

generally *Ashwander v. TVA*, 297 U.S. 288, 348 (1936) (Brandeis, J.,concurring). As noted above, and in our principal brief, that interpretation is the correct one and flows from the plain language of the provisions and the legislative history. See *Almendarez-Torres v. United States*, 523 U.S. 224, 238 (1998)(doctrine applies only where the statute is "genuinely susceptible to two constructions after, and not before, its complexities are unraveled"). Moreover, Congress enacted this legislation aware of the constitutional issues it raised and set forth a strong case for its constitutionality. The 1978 Senate Intelligence Report expressly contemplated that FISA would be used for law enforcement purposes, and understood that "[t]he targeting of U.S. persons [in foreign counterintelligence and counterterrorism investigations] and the overlap with criminal law enforcement require close attention to traditional fourth amendment principles." S. Rep. No. 95-701, 95th Cong., 2d Sess. 11 (1978) [hereinafter Senate Intelligence Report]. But Congress concluded that such use of FISA would in fact be constitutional. See id. at 11-16.

Members of Congress understood that the USA Patriot Act could also raise constitutional questions, but intended for the courts to resolve the meaning of the statute as written. See 147 Cong. Rec. S10589 (Oct. 11, 2001) (statement of Senator Edwards); id. at S10593 (statement of Senator Cantwell). Indeed, Senator Leahy discussed the constitutional questions raised by the two USA Patriot Act amendments together. He observed that under the coordination amendment, "[p]rotection against these foreign-based threats [terrorism and espionage] by any lawful means is within the scope of the definition of 'foreign intelligence information,' and the use of FISA to gather evidence for the enforcement of these laws" has always been permitted. He also noted that the USA Patriot Act "adopts 'significant purpose,' and it will be up to the courts to determine how far law enforcement agencies may use FISA for criminal investigation and prosecution beyond the scope of the statutory definition of 'foreign intelligence information.'" 147 Cong. Rec. S11004 (Oct. 25, 2001) (emphasis added). This reflects an understanding that (1) the coordination amendment reaffirmed the broad definition of "foreign intelligence information" to include evidence sought for certain prosecutions; (2) the significant purpose amendment allowed FISA to be used primarily for a purpose other than collection of foreign intelligence information as so defined; (3) the two amendments would be applied together; and (4) whatever constitutional questions the amendments raised would have to be resolved by the courts.[7]

[7] In a hearing on September 10, 2002 (copy of transcript attached), Senator Leahy stated:

> I was surprised to learn that as, quote "The drafter of the coordination amendment" close quote, of the USA Patriot Act, the [Department of Justice] cites my statement - cites a Leahy

> statement to support its argument that there is no longer a distinction between using FISA for a criminal prosecution and using it to collect foreign intelligence. Had the Department of Justice taken the time to pick up a phone and call me, and incidentally I have a listed phone number, both home and at the office, I would have told them that was not, and is not, my belief.
>
> On September 24, 2002, Senators Hatch, Thurmond, Kyl, DeWine, Sessions, and McConnell inserted into the Congressional record a statement that the Patriot Act was designed to allow "'our law enforcement and intelligence communities * * * to cooperate fully in protecting our Nation against terrorist attacks,'" and asserting that "[i]t was our intent * * * to change FISA to allow a foreign intelligence surveillance warrant to be obtained even when the primary purpose of the surveillance was the gathering of criminal evidence." See footnote 2, supra.

Indeed, because the President has the inherent constitutional authority to conduct warrantless intelligence surveillance based on a significant foreign intelligence purpose, this Court must interpret FISA to avoid infringement of this presidential power, if possible. Thus, it is the FISC's interpretation of FISA and the USA Patriot Act, not the government's, that raises the more severe constitutional questions. To the extent that avoidance doctrine governs here, it Compels the Court to read the statute to support, rather than infringe, the President's constitutional power and responsibility to keep the country safe.

CONCLUSION

It is respectfully submitted that the judgment of the FISC in this case, including its adoption of the opinion and order of May 17, 2002, and its new Rule 11, should be vacated, and the case remanded with directions to the FISC to grant the FISA application as submitted.

[signed: John Ashcroft]
JOHN ASHCROFT
Attorney General

LARRY D. THOMPSON
Deputy Attorney General

THEODORE B. OLSON
Solicitor General

DAVID S. KRIS
Associate Deputy Attorney General

JAMES A. BAKER
Counsel for Intelligence Policy

JONATHAN L. MARCUS
Attorney Advisor
Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
(202)514-2882

Dated: September 25, 2002

APPENDIX: COMPARISON OF FISA AND TITLE III

At the hearing on September 9, this Court inquired into the differences between FISA and Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-2522. Set forth below is a detailed comparison between the two statutes in the following areas: (1) review by a neutral and detached magistrate, (2) probable cause, (3) particularity, (4) necessity, (5) duration of surveillance, (6) minimization, (7) sealing, (8) notice to the target, (9) suppression, and (10) other matters. As the discussion demonstrates, FISA is more flexible than Title III in some, but not all, of these areas. Moreover, the differences between the two statutes are not always of constitutional significance - particularly where, as in this case, FISA is applied to U.S. persons who are "agents of a foreign power" under the rubric of international terrorism, 50 U.S.C. § 1801(b)(2)(C) and (E).[1]

1 Based in part on *Berger v. New York*, 388 U.S. 41 (1967), the courts of appeals have generally held that the Constitution governs the first six of the 10 areas listed above. See *United States v. Williams*, 124 F.3d 411, 416 n.5 (3d Cir. 1997);*United States v. Falls,* 34 F. 3d 674 (8th Cir. 1994); *United States v. Koyomejian*, 970 F.2d 536 (9th Cir. 1992) (en banc); *United States v. Mesa-Rincon*, 911 F.2d 1433 (10th Cir. 1990 ; *United States v. Biasucci*, 786 F.12d 504 (2d Cir. 1986);*United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987); *United States v. Torres*, 751 F. 20 875 (7th Cir. 1984). We do not necessarily agree with all aspects of those decisions. We do agree, however, with cases holding that other areas of difference between FISA and Title III are not constitutionally significant. See *United States v. Ianiello*, 621 F. Supp. 1455, 1468-1469 (S.D.N.Y. 1985).

It is important to note that the discussion below compares the statutory language of FISA and Title III. As applied in particular cases, similar language may produce different results. For example, as explained in Section (5), infra, both FISA and Title

III give the supervising court discretion to require periodic reports on the progress of electronic surveillance. Compare 50 U.S.C. § 1805(e)(3), with 18 U.S.C. § 2518(6). As a practical matter, many Title III courts require 10-day progress reports; the same is not true of the FISC. See Senate Five Year Report at 11; see also footnote 6, infra. The argument here is not that FISA's discretionary provisions are (or should be) applied in accord with Title III, or that such application is necessary to avoid constitutional questions. On the contrary, FISA should be interpreted and applied in keeping with its purpose requirements, which also support its constitutionality. Particularly in a case like the present one, however, the differences between FISA and Title III are not as significant as they might appear to be.

1. Review By A Neutral and Detached Magistrate.

With limited exceptions, both FISA and Title III require the government to file an application for a court order authorizing electronic surveillance. 50 U.S.C. § 1804; 18 U.S.C. § 2518. Both statutes thus satisfy the constitutional requirement that warrants must be issued by neutral, disinterested magistrates." *Dalia v. United States*, 441 U.S. 238, 255 (1979); see House Report 23 (noting the three exceptions in FISA to the requirementof a "prior judicial warrant"); *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (Kennedy, J.) (holding that the FISC is a "neutral and detached" court).

2. Probable Cause.

Both Title III and FISA require the government to establish, and the court to find, probable cause justifying the use of electronic surveillance. Under title III, the court must find "on the basis of the facts submitted by the applicant that * * * there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of thie chapter." 18 U.S.C. § 2518(3)(a). For wire and oral communications (e.g., telephone and microphone interception), Section 2516 enumerates a long list of predicate offenses, ranging from bank fraud (18 U.S.C. § 1344)to unlawful possession of a firearm (18 U.S.C. S 922(g)), and including espionage (e.g., 18 U.8.C. § 794), assassination (e.g.,18 U.S.C. §§ 351, 1751), sabotage (e.g., 18 U.S.C. § 2155), terrorism (e.g., 18 U.S.C. § 2332), and aircraft piracy (49 U.S.C. § 46502). For electronic communications (e.g., electronic mail or facsimile messages under Title III), any federal felony may serve as a predicate. 18 U.S.C. § 2516(3). Title III requires probable cause only that "an individual" is committing a predicate offense, and the court may grant a Title III application even if the government is unable to identify the individual whose communications are to be intercepted or who is committing the predicate offense. See *United States v. Kahn*, 415 U.S. 143, 157 (1974) ("when there is probable cause to believe that a particular telephone is being used to commit an offense but no

particular person is identifiable, a wire interception order may, nevertheless, properly issue under the statute").[2]

> [2] Section 2518(l)(b)(iv) requires every Title III application to include "a full a complete statement * * * including * * * the identity of the person, if known, committing the offense and whose communications are to be intercepted." Every Title III order must specify "the identity of the person, if known, whose communications are to be intercepted." 18 U.S.C.2518(4)(a).

In contrast, FISA requires the court to find, "on the basis of the facts submitted by the applicant," that "there is probable cause to believe that * * * the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States." 50 U.S.C. § 1805(a)(3).[3]

> [3] A FISA application must include "the identity, if known, or a description of the target of the electronic surveillance." 50 U.S.C. § 1804(a)(3). Orders authorizing electronic surveillance must specify "the identity, if known, or a description of the target of the electronic surveillance." 50 U.S.C. § 1805(c)(1)(A). Cf. House Report 73.

The terms "foreign power" and "agent of a foreign power" are defined by FISA in ways that sometimes, but not always, require a showing of criminal conduct.

Under FISA, a "foreign power" is defined to be any of the following (50 U.S.C. § 1801(a)):

> (1) a foreign government or any component thereof, whether or not recognized by the United States;
>
> (2) a faction of a foreign nation or nations, not substantially composed of United States persons;
>
> (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;
>
> (4) a group engaged in international terrorism or activities in preparation therefor;
>
> (5) a foreign-based politica1 organization, not substantially composed of United States persons; or

(6) an entity that is directed and controlled by a foreign government or governments.

Five of these six definitions can be satisfied without any showing of criminal activity. For example, a foreign government, whether friendly or hostile to the United States, is a "foreign power" under Section 1801(a)(1). See House Report 29.

The fourth definition, which refers to "international terrorism" and which is applicable to this case, does require criminal conduct. See House Report 30 ("The term 'international terrorism' is a defined term * * * and includes within it a criminal standard"). FISA defines "international terrorism" to require, among other things, "activities that * * * involve 'violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State." 50 U.S.C. § 1801(c). Thus, while the definition extends to terrorist acts abroad, those acts must be of a sort that would be criminal if committed in the United States - e.g., bombing the Eiffel Tower instead of the World Trade Center. See House Report at 42, 45.

A group may also be a "foreign power" under the fourth definition if it engages in "activities in preparation" for international terrorism. The "preparation therefor" standard may or may not be more expansive than the criminal "attempt" standard, which is generally understood to require a "substantial step" towards completion of an offense, see *Braxton v. United States,* 500 U.S. 344, 351 (1991); House Report 43, but it is surely no broader than the "overt act" requirement of some criminal conspiracy statutes, such as 18 U.S.C. § 371, see *United States v. Shabani*, 513 U.S. 10, 14 (1994). A "group" engaged in preparatory activities for international terrorism would, of course, satisfy criminal conspiracy standards. See ibid.

The term "agent of a foreign power" is defined by FISA as follows (50 U.S.C. § 1801(b)):

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

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

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

person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

any person who

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

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

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

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

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

This definition distinguishes between "United States persons" and other persons. A "United States person" is defined by FISA to be "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power as defined in subsection (a)(1), (2), or (3) of this section." In practical terms, therefore, a "U.S. person" under FISA is a U.S. citizen or a permanent resident alien (green card holder); visiting foreigners and illegal aliens are not "U.S. persons." See House Report 32.

A U.S. person can be an "agent of a foreign power" only if he engages in some level of criminal activity. There are two main categories of U.S. person agents of foreign powers: The first category includes persons engaged in espionage and clandestine intelligence activities; the second category includes persons engaged in sabotage and international terrorism. A third category, that is not as significant as the first two, includes persons who enter the United States under a false identity. Eachcategory is discussed below.

A U.S. person who is engaged in "clandestine intelligence gathering activities" or "other clandestine intelligence activities" for or on behalf of a foreign power may be an agent of that foreign power only if those activities either "involve," "may involve," or "are about to involve" a "violation of the criminal statutes of the United States." 50 U.S.C. § 1801(b)(2)(A)-(B); see House Report 39. By setting a "may involve" standard, Congress intended to require less than the showing of probable cause applicable in ordinary criminal cases. See House Report 39-40, 79.

To be an "agent of a foreign power" under the rubric of international terrorism or sabotage, a U.S. person must "knowingly engage[]" in "sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power." 50 U.S.C. 5 1801(b)(2)(C). The term "sabotage" is defined to mean "activities that involve a violation of chapter 105 of Title 18, or that would involve such a violation if committed against the United States." 50 U.S.C. § 1801(4). Thus, like international terrorism, sabotage is defined to require activity that is criminal or would be criminal if the United States were directly involved. The U.S. person must actually be "engage[d] in" sabotage or international terrorism or activities in preparation therefor - i.e., committing or preparing to commit the specified acts.

A U.S. person may also be an "agent of a foreign power" if he knowingly aids and abets or conspires with others engaged in clandestine intelligence activities or sabotage/international terrorism. 50 U.S.C. § 1801(b)(2)(E). These are criminal law standards. Compare 18 U.S.C. §§ 2, 371. As the House Report explains (at page 44), "[t]his standard requires the Government to establish probable cause that the prospective target knows both that the person with whom he is conspiring or whom he is aiding and abetting is engaged in the described activities as an agent of a foreign power and that his own conduct is assisting or furthering such activities. The innocent dupe who unwittingly aids a foreign intelligence officer cannot be targeted under this provision."

Finally, a U.S. person may also be an "agent of a foreignpower" if he "knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power." 50 U.S.C. § 1801(b)(2)(D). This

provision requires knowingly false or fraudulent conduct, and will almost always involve a crime, because - apart from the specific requirements of the customs and immigration laws - it is not possible legally to enter this country without providing proof of identity to a federal official. See 18 U.S.C. § 1001 (making it a crime to provide a false statement to a federal official); *United States v. Popow*, 821 F.24 483, 485 (8th Cir. 1987) ("We hold that the giving of a false identification at the United States border is punishable under § 1001 because it is both material and within the jurisdiction of a federal agency"). Similarly, assuming a false identity in the United States for or on behalf of a foreign power will almost inevitably result in a fraud offense of one sort or another. For example, the provision would not include a person who assumes a false identity to escape an abusive spouse, or even to evade a creditor.

Thus, a U.S. person may not be an "agent of a foreign power" unless he engages in activity that either is, may be, or would be a crime if committed against the United States or within U.S. jurisdiction. Although FISA does not always require a showing of an imminent crime or "that the elements of a specific offense exist," Senate Intelligence Report at 13, it does require the government to establish probable cause to believe that an identifiable target is knowingly engaged in terrorism, espionage, or clandestine intelligence activities or is knowingly entering the country with a false identity or assuming one once inside the country on behalf of a foreign power. Thus, while FISA imposes a more relaxed criminal probable cause standard than Title III, those differences are not extensive as applied to U.S. persons.

Of particular relevance in this case, the differences in the area of international terrorism are slight to the point of vanishing - the only significant variance being that FISA extends to terrorist activity overseas (and outside U.S. jurisdiction) as well as within the United States. For obvious reasons, there is little case law concerning the application of the Fourth Amendment to international terrorism outside U.S. criminal law jurisdiction. However, virtually any U.S. person located in this country who is an "agent of a foreign power" under the rubric of international terrorism would likely be violating a U.S. law, even if he planned to commit terrorist acts outside U.S. jurisdiction. For example, under 18 U.S.C. § 956(a), it is a crime for any person

> within the jurisdiction of the United States, [to] conspire[] with one or more other persons, regardless of where such other person or persons are located, to commit at any place outside the United States an act that would constitute the offense of murder, kidnapping, or maiming if committed in the special maritime and territorial jurisdiction of the United States * * * if any of the conspirators commits an act within the jurisdiction of the United States to effect any object of the conspiracy.

Section 956(b) applies the same standards to conspiracies to "damage or destroy specific property situated within a foreign country and belonging to a foreign

government or to any political subdivision thereof with which the United States is at peace, or any railroad, canal, bridge, airport, airfield, or other public utility, public conveyance, or public structure, or any religious, educational, or cultural property so situated." Because a U.S. person terrorist Under FISA must be working "for or on behalf" of an international terrorist group, he would appear to satisfy the conspiracy elements of Section 956.[4]

[4] In addition, Section 2331 of Title 18 defines "international terrorism" almost exactly as FISA does, and numerous provisions of Title 18 make criminal various activities in connection with terrorist acts that occur outside the UnitedStates. See, e.g., 18 U.S.C. §§ 2332d (engaging in a financial transaction with a country designated as a supporter of international terrorism); 2332f (delivering or detonating an explosive or other lethal device in, into, or against a place of public use); 2339A (providing material support or resources knowing that they are to be used in preparing for or carrying out, inter alia, destruction of aircraft; violent acts at international airports; possession of biological weapons; possession of chemical weapons; possession of nuclear material without lawful authority; or conspiracy to injure persons or damage property in a foreign country); 2339B (providing material support or resources to a foreign terrorist organization); 2339C (willfully providing or collecting funds with knowledge or intention that funds are to be used to carry out, inter alia, any act intended to cause death or serious bodily injury to a civilian when the purpose of such act is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act).

Moreover, under 28 U.S.C. § 1782 and various Mutual Legal Assistance Treaties (MLATs), the United States has authority to conduct searches and/or subpoena information on behalf of foreign governments based on suspected violations of foreign laws. Cf., e.g., *In re Request from Canada Pursuant to Treaty Between the U.S. and Canada on Mutual Legal Assistance in Criminal Matters*, 155 F. Supp.2d 515 (M.D.N.C. 2001); Treaty with the United Kingdom on Mutual Legal Assistance on Criminal Matters, Jan. 6, 1994, S. Treaty Doc. No. 104-2, 1994 WL 855115.

On the other side of the balance, FISA's terrorism standards require more than Title III in several respects. First, of course, the probable cause that is required is probable cause to believe not merely that a simple violation of law has been committed, see *Whren v. United States*, 517 U.S. 806, 815 (1996), but probable cause to believe that the target has engaged in particularly serious crimes - i.e., those that involve

"violent acts or acts dangerous to human life." Cf., *Brinegar v. United States*, 338 U.S. 160, 182-183 (1949) (Jackson, J., dissenting). FISA applies to a far narrower range of criminal conduct than Title III. Compare 50 U.S.C. § 1801 with 18 U.S.C. § 2516.

Second, not only must the government satisfy the criminal elements of international terrorism, it must also show that the terrorism offense is being committed "for or on behalf of" an international terrorist group. That provision requires "the Government to show a nexus between the individual and the foreign power that suggests that the person is likely to do the bidding of the foreign power." House Report at 35 (discussing the identical phrase in the context of clandestine intelligence activities). The government must show that the terrorist activity is transnational in some way - e.g., because the "perpetrators operate or [plan to] seek asylum" abroad.

Third, under FISA's definition of international terrorism, the government must also show that the violent acts appear to be intended either to "intimidate or coerce" a government or a civilian population, or to affect government conduct "by assassination or kidnapping." As the House Report explains (at page 45):

> Examples of activities which in and of themselves would meet these requirements would be: the detonation of bombs in a metropolitan area, the kidnapping of a high-ranking government official, the hijacking of an airplane in a deliberate and articulated effort to force the government to release a certain class of prisoners or to suspend aid to a particular country, the deliberate assassination of persons to strike fear into other to deter them from exercising their rights of the destruction of vital government facilities. Of course, other violent acts might also satisfy these requirements if the requisite purpose is demonstrated.

In sum, as applied to U.S. person terrorists, FISA requires more than mere probable cause to believe a crime has been committed. It applies only to a small set of extremely serious crimes, and only when those crimes are committed on behalf of a foreign power and involve international activity. FISA cannot be used to monitor a U.S. person merely because he works as in-house counsellor as a registered lobbyist for a foreign government, see House Report 30, 32, and it cannot be used to monitor the vast majority of criminals, from corrupt business executives (e.g., Enron management), to members of organized crime families (e.g., John Gotti), to domestic terrorists (e.g., Timothy McVeigh). See id. at 30 (where necessary, "groups engaged in terrorism of a purely domestic nature * * * should be subjected to surveillance under" Title III, not FISA). Thus, in its probable cause provisions, FISA is more demanding than Title III when applied to U.S. person terrorists.

3. Particularity (Nexus to Surveilled Facility).

Title III and FISA impose different requirements concerning the nexus between the target's activity and the scope of the surveillance. There are two main differences. First, under Title III, the government must establish, and the court must find, that "there is probable cause for belief that particular communications concerning [the specified predicate] offense will be obtained through [the] interception." 18 U.S.C. § 2518(3)(b). The closest analog in FISA is the requirement that a high-ranking Executive Branch official designate the type of foreign intelligence information being sought (e.g., information "necessary to[] the ability of the United States to protect against * * * actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power," 50 U.S.C. § 1801(e)(1)(A)), and certify "that the certifying official deems the information sought to be foreign intelligence information." 50 U.S.C. § 1804(a)(7)(A). This certification is reviewed for clear error when the target of the surveillance is a United States person. (No review is conducted in other cases.) 50 U.S.C. § 1805(a)(5); House Report at 80-81.[5]

[5] The House Report states that "[t]he 'clearly erroneous' standard of review is not, of course, comparable to a probable cause finding by the judge. Nevertheless, this bill does provide a workable procedure for judicial review (and possible rejection) of executive branch certifications for surveillances of U.S. persons." House Report at 80.

Second, absent authorization for so-called "roving" surveillance, see 18 U.S.C. § 2518(11), Title III requires "probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of the [specified predicate] offense, or are leased to, listed in the name of, or commonly used by such person." 18 U.S.C. § 2518(3)(d). By contrast, FISA requires only that the court find probable cause that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C.§ 1805(a)(3)(B).

These different legal standards are insignificant in practical terms. As to the first requirement, the Executive Branch must certify under FISA that it is seeking pertinent information (foreign intelligence information), and whether or not there is judicial review of that certification, the government is not permitted to submit a false certification. The certification typically comes from the Director of the FBI, and every FISA application is approved by the Attorney General or Deputy Attorney General. See 50 U.S.C. §§ 1804(a), 1804(a)(7); see also *United States v. Bianco*, 998 F.2d 1112, 1124 (2d Cir. 1993) (requiring high-ranking official to authorize surveillance is "protection[] against arbitrary surveillance"). Thus, in practical effect, FISA's standards are not very different from Title III's requirement that the government show, and the court find, probable cause that pertinent communications will be obtained by the surveillance.

As to the second requirement, most facilities subjected to electronic surveillance under Title III and FISA alike are in fact "leased to, listed in the name of, or commonly used by" the target. 18 U.S.C. § 2518(3)(d). In such cases, Title III is no more difficult to satisfy than FISA. In the unusual case where they are not so leased, listed, or commonly used, Title III requires the government to show a nexus between the facilities and communications regarding the criminal offense, a standard that may delay the onset of surveillance for additional investigation, but which will not often prevent it.[6]

[6] For prudential reasons, the Department in practice is often cautious about using the "listed, leased, or commonly used" provision of Title III absent evidence that the facility is in fact being used in connection with the predicate offense.

In any event, Title III's more rigorous nexus requirements are counterbalanced by its more relaxed requirements concerning the identity of the surveillance target. As noted above, Title III does not require the government to show, or the court to find, anything about the target of the surveillance; it is enough that "an individual" is committing a predicate offense. 18 U.S.C. § 2518(3)(a); see Kahn, supra. Given that expansive approach, rigorous nexus requirements are understandable. By contrast, FISA requires probable cause to believe the target is an agent of a foreign power who uses or is about to use the targeted facility. Thus, while FISA requires less of a nexus between the facility and pertinent communications, its requires more of a nexus between the target and pertinent communications. See House Report at 73. In the end, therefore, both FISA and Title III provide reasonable assurance that the surveillance will be directed at pertinent communications. Cf. *Dalia*, 441 U.S. at 255-256 (Fourth Amendment particularity standard requires that warrant describe the things to be seized and the place to be searched but does not require specification of the means by which search will be executed).

4. Necessity.

Title III and FISA contain similar "necessity" requirements. Every Title III application must provide "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(l)(c). Correspondingly, the issuing court under Title III must find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(3)(c).

FISA's "necessity" provision requires a high-ranking Executive Branch official to certify that the information sought by electronic surveillance "cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. § 1804(a)(7)(B)(ii). This certification is reviewed for clear error when the target of the surveillance is a United

States person. (No review is conducted in other cases.) 50 U.S.C. § 1805(a)(5); House Report at 80-81. Neither FISA nor Title III requires "probable cause" of necessity; instead, both contemplate judicial review of a statement of necessity from the government. Under FISA, that statement is reviewed for clear error, while under Title III it is reviewed without deference. In that respect, FISA is more favorable to the government. However, while the statement of necessity in a Title III application comes from the applicant - typically a line agent or attorney - the certification of necessity in a FISA application comes from the Director of the FBI or a similar official. The deferential standard of review is appropriate in light of the stature of such an official.

5. Period of Surveillance Order.

Title III provides for shorter periods of surveillance than FISA. Under Title III, authorization orders are issued for periods of up to 30 days. 18 U.S.C. 2518(5). Under FISA, authorization orders are issued for periods of up to 90 days for U.S. persons. 50 U.S. C. § 1805 (e)(1).[7]

[7] For non-U.S. persons who are "agents or employees" of a foreign power or "members" of an international terrorist group, initial surveillance orders may be for up to 120 days, and renewal orders for up to one year. 50 U.S.C. § 1805(e)(l)-(2). Certain foreign powers themselves, as opposed to their agents, are also subject to longer periods of surveillance. Ibid.

Thus, in cases involving a U.S. person, the government must obtain three Title III orders for every one FISA order. But that is primarily an administrative burden rather than a legal one. Although shorter maximum time periods ensure regular judicial review of the progress of Title III surveillance, FISA does not require the FISC in every case to allow surveillance for the full 90 days, and the statute allows the FISC to "assess compliance with the minimization procedures" either "[a]t or before the end of the period of time for which electronic surveillance is approved by an order or an extension." 50 U.S.C. § 1805(e)(3); cf. 18 U.S.C.§ 2518(6) (authorizing the Title III judge to require the filing of regular progress reports). In our view, there is no constitutional significance to the difference in the allowable duration of orders under FISA and Title III in cases involving U.S. persons.

6. Minimization.

FISA and Title III have different minimization regimes. The minimization provisions in FISA are "meant generally to parallel the minimization provision in [Title III]," but are not "as strict" as those in Title III with respect to the acquisition of information. S. Rep. No. 95-604, 95th Cong., 1st Sess. 37 (1977) [hereinafter Senate Judiciary Report], House Report at 56. In particular, FISA allows greater flexibility, not only in

respect to what may be acquired but also in the means used to acquire it. FISA only requires the minimization of information concerning U.S. persons. See 50 U.S.C. § l801(h)(1). Moreover, under FISA,the recording devices are normally (but not always) left on, and minimization occurs in the process of indexing and logging the pertinent communications. See FISC May 17, 2002 Order at 11. (We are lodging with the Court the FBI's classified Standard Minimization Procedures.) Under Title III, such an approach is used only when the communications are in code or a foreign language for which there is no contemporaneously available translator (which often is the case with respect to FISA targets), and even then minimization must take place as soon as practicable. 18 U.S.C. § 2518(5). FISA's more flexible procedures nevertheless ensure that information about a U.S. person is neither retained nor disseminated unless it is foreign intelligence or evidence of an ordinary crime. Given that FISA targets hostile activities by foreign powers and their agents that by their very nature will often involve multiple actors and complex plots, as well as foreign languages and codes, less minimization in the acquisition stage is justified. See *Scott v. United States*, 436 U.S. 128, 140 (1978) ("when the investigation is focusing on what is thought to be a widespread conspiracy, more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise.").[8]

[8] Moreover, as explained in the discussion of "sealing," infra, FISA's minimization provisions are stricter than those in Title III because they regulate not only the acquisition, but also the retention and dissemination of information. See House Report 56.

7. Sealing.

Unlike FISA, Title III contains a sealing requirement. Under 18 U.S.C. § 2518(8)(a), the tape recordings of intercepted communications are to be sealed "[i]mmediately upon the expiration of the period of the order, or extensions thereof." The purpose of the sealing requirement is to preserve the integrity of the electronic surveillance evidence. See *United States v. Ojeda-Rios*, 495 U.S. 257 (1990). Section 2518(8)(a) contains an explicit exclusionary remedy for failure to comply with the sealing requirement or to provide a "satisfactory explanation for the absence" of a seal.

By contrast, FISA contains no analogous sealing requirement, although it does require the government to retain FISA applications and orders for 10 years. 50 U.S.C. § 1805(h). In part because Congress (correctly) predicted that FISA information would rarely be used in a criminal prosecution, it concluded that ordering the government to retain all information acquired would not be the best way to protect privacy. On the contrary, Congress concluded that privacy would be best protected by requiring the governing in certain cases not to retain information, but to destroy it. House Report 56. Accordingly, as the House Report explains, "while (Title III] does not require minimizing retention and dissemination, this bill does," and may in certain instances

require "destruction of unnecessary information acquired." ibid. The Constitution does not require sealing of intercepted communications. See *United States v. Ianiello*, 621 F. Supp. 1455, 1468-1469 (S.D.N.Y. 1985).

8. Notice to the Target.

Under Title III, the target of electronic surveillance (and other persons within the discretion of the district judge) must be notified of surveillance when it expires. 18 U.S.C. § 2518(o)(d). The court has discretion to provide to the target or his counsel "portions of the intercepted communications, applications and orders." Ibid. Upon an ex parte showing of good cause by the government the notice may be postponed, but it must eventually be provided. Ibid. By contrast, FISA requires notice to a person whose communications were intercepted if and only if the government "intends to enter into evidence or otherwise use or disclose [the communications, or information derived from the communications] in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States." 50 U.S.C.§ 1806(c). That is a significant difference because many FISA surveillances do not result in the use of communications in any proceeding. However, to the extent that courts are concerned about increased use of FISA for law enforcement purposes, notice to the target is required before FISA-derived information is used in court. And to the extent FISA is not used for law enforcement, the justification for not notifying the target - to maintain the secrecy of the intelligence investigation - is compelling. See Senate Intelligence Report at 12 ("The need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement").

9. Suppression Remedy.

Under 18 U.S.C. § 2518(9) (governing admission of Title III evidence in any trial or proceeding), and standard criminal discovery rules, a defendant moving to suppress information obtained or derived from Title III is entitled to see the Title III applications and orders, although in rare cases some redactions may be ordered. See, e.g., *United States v. Danovaro*, 877 F.2d 583 (7th Cir. 1989). Under FISA, by contrast, the defendant normally does not see the FISA application or orders. Under FISA, "notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States," the district court must "review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted." 50 U.S.C. § 1806(f). The court is authorized to disclose the FISA application to the defendant "only where such disclosure is necessary to make an

accurate determination of the legality of the surveillance" or when otherwise required by due process. Ibid.; 50 U.S.C. § 1806(g).

FISA nevertheless provides for a case-by-case evaluation of whether disclosure might be required, and the Supreme Court has never held that disclosure of surveillance materials is mandatory, even with respect to ordinary law enforcement, in order for the district court to determine the legality of the surveillance. See *Giordano v. United States*, 394 U.S. 310, 313 (1969) (per curiam) ("Of course, a finding by the District Court that the surveillance was lawful would make disclosure and further proceedings unnecessary."); *United States v. Butenko*, 494 F.2d 593, 607 (3d Cir. 1974) ("Since the question confronting the district court * * * was the legality of the taps, not the existence of tainted evidence, it was within his discretion to grant or to deny Ivanov's request for disclosure and a hearing."); cf. *Alderman v. United States*, 394 U.S. 165, 180-186 (1969) (disclosure of surveillance materials required when and if court finds surveillance violated defendant's Fourth Amendment rights, so that defendant may argue for exclusion of evidence tainted by illegal surveillance). Thus, FISA's flexible discovery standards satisfy the Constitution; their application in any particular case would, of course, depend on the facts.

10. FISA's Unique Safeguards.

There are at least two ways in which Congress made FISA more demanding than Title III to "provide[] safeguards that have not existed before and that may reasonably be expected to prevent any recurrence of the abuses of the past." Senate Intelligence Report at 16.

First, FISA requires the certification of the FBI Director (or other, similar official), the personal approval of the Attorney General or the Deputy Attorney General, and review of the high-level certification by an Article III judge. In contrast, a Deputy Assistant Attorney General (a member of the Senior Executive Service who is not subject to Senate confirmation and who is one rank below an Assistant Attorney General) may approve a Title III application for wire or oral communications. 18 U.S.C. § 2518(l). (For roving or emergency applications, Title III requires the approval of a higher-ranking official. See 18 U.S.C. § 2518(7), (11)). And Title III permits any attorney for the government to apply for an order authorizing interception of electronic communications. 18 U.S.C. § 2516(3). FISA's certification and approval requirements serve as a check against abuse of powers by ensuring that the highest Executive branch officials are personally accountable for the electronic surveillance and physical searches conducted under their signatures, see *Bianco*, 998 F.2d at 1124, and the judicial review requirement serves as an additional check against use of FISA for illegitimate reasons.

Second, FISA contains far more extensive reporting requirements than Title III. Where Title III requires only an annual report containing "a general description" of surveillances and certain statistical information, 18 U.S.C. § 2519(2), FISA requires the Executive Branch to keep the Intelligence Committees "fully informed," in keeping with the general framework for intelligence oversight. 50 U.S.C. §§ 1808(a)(1), 1826. Congress similarly believed that its "close and continuing" oversight would "suppl[y] a compensating check" against potential Executive Branch abuses. Senate Intelligence Report at 11-12. In addition, by providing for the sunset of the amendments to FISA in the USA Patriot Act, Congress has made clear its intention to hold the Executive Branch accountable for the exercise of its FISA authority. See Section 224(a) of the USA Patriot Act, Pub.L. No. 1107-56, 115 Stat. 272 (Oct. 26, 2001).
