ELECTRONIC SURVEILLANCE OF TERRORISM: THE INTELLIGENCE/LAW ENFORCEMENT DILEMMA—A HISTORY

by
William Funk[*]

The Foreign Intelligence Surveillance Act (FISA) has been much in the news. Because the requirements for a judicial warrant under FISA do not require the traditional showings for electronic surveillance for law enforcement purposes, one of the issues relating to FISA is the extent to which surveillance under that Act may be undertaken for the purposes of criminal law enforcement, rather than for obtaining foreign counterintelligence or counterterrorism information. This issue became particularly salient after 9/11 when at the administration's urging Congress passed an amendment to FISA in the USA PATRIOT Act that eliminated the previous requirement that "the purpose" of the surveillance was to obtain foreign intelligence information and replaced it with the requirement that "a significant purpose" be to obtain such information.

This Article traces the history of FISA's adoption and subsequent practice to show that the original intent of FISA, recognized by the government and confirmed by the courts, was that the primary purpose for the surveillance had to be the gathering of foreign intelligence, including intelligence concerning international terrorism, rather than obtaining evidence for use in criminal trials. The Article then describes how FISA was later misconstrued by employees in the Justice Department, and later by the Foreign Intelligence Surveillance Court, to erect a so-called wall between intelligence and law enforcement officers that was not only not required by FISA but contrary to its purpose and history. Some have attributed much of the blame for the 9/11 intelligence failure to the existence of this "wall," creating a perceived need to amend FISA to eliminate the wall through the amendment of the "purpose" requirement in the USA PATRIOT Act. This Article demonstrates how that amendment was unnecessary and suggests that the amendment raises other constitutional issues with respect to FISA.

[*] Professor of Law, Lewis & Clark Law School. During the period 1974–1977, I was an attorney in the Office of Legal Counsel in the Department of Justice, where my principal responsibilities related to intelligence matters. As such, I was intimately involved in the drafting of the original versions of FISA and in the reports of the Senate Judiciary and Intelligence Committees. I was recruited by the House Permanent Select Committee on Intelligence to come to that committee to aid in its consideration of FISA in 1977. There I was the principal staff person on the Legislation Subcommittee, the subcommittee responsible for consideration of the FISA bill.

I. INTRODUCTION

The events of 9/11, like the attack on Pearl Harbor, occasioned several substantial investigations into the supposed intelligence failures that allowed such surprise attacks to occur.[1] One of the putative findings with respect to 9/11 was that there existed a "wall" between law enforcement and intelligence agencies that impeded the sharing of information between them.[2] Even before those findings were made, however, there was already a perception by some that this wall was fostered or reinforced both by provisions of the Foreign Intelligence Surveillance Act[3] (FISA), the law authorizing electronic surveillance for foreign intelligence purposes, and by the manner in which it was administered.[4] In particular, one provision in FISA was identified as needing amendment.[5] That provision required high government officials to certify that "*the purpose* of the surveillance is to obtain foreign intelligence information"[6] in order to obtain a court order authorizing such a surveillance. One might infer from this language that criminal law enforcement could not be the purpose of the surveillance. Moreover, the Administration apparently believed that this provision required a

[1] *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 339–60 (2004) [hereinafter 9/11 COMMISSION REPORT], *available at* http://www.gpoaccess.gov/911/pdf/fullreport.pdf (investigatory account of failures leading up to 9/11 attack, replete with comparisons to failures and lessons surrounding attack on Pearl Harbor).

[2] *Id.* at 78, 79 (overview of different methods used for law enforcement and intelligence as well as problems inherent in sharing information among agencies). *See also* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS 21–42, *available at* http://cybersafe.gov/oig/special/0506/final.pdf (description and history of "the wall").

[3] Heather Mac Donald, *Why the FBI Didn't Stop 9/11*, CITY J., Autumn 2002, at 14, *available at* http://www.city-journal.org/html/12_4_why_the_fbi.html.

[4] *See, e.g.*, U.S. DEP'T OF JUSTICE, FINAL REPORT OF THE ATTORNEY GENERAL'S REVIEW TEAM ON THE HANDLING OF THE LOS ALAMOS NATIONAL LABORATORY INVESTIGATION 714–15 (May 2000) [hereinafter BELLOWS REPORT], http://www.usdoj.gov/ag/readingroom/bellows.htm; *see also* George Lardner Jr., *Report Criticizes Stumbling Block Between FBI, Espionage Prosecutors*, WASH. POST, Dec. 13, 2001, at A3 (summary of Bellows Report reveals shift in procedure).

[5] *See* 9/11 COMMISSION REPORT, *supra* note 1, at 78–79.

[6] Foreign Intelligence Surveillance Act, 50 U.S.C. § 1804(a)(7)(B) (1982) (emphasis added). This is not, of course, the only requirement for obtaining an order authorizing electronic surveillance to obtain foreign intelligence information, but it is a necessary condition.

surveillance under FISA to have a "sole or primary purpose" of obtaining foreign intelligence, rather than a purpose of obtaining evidence for use in a criminal enforcement action.[7] Consequently, the Administration sought and received an amendment to this provision in the USA PATRIOT Act.[8] That new and current provision[9] now provides that the certification state that "*a significant purpose* of the surveillance is to obtain foreign intelligence information."[10] The intent of this change was to establish that a FISA surveillance could be utilized for the express purpose of gathering evidence of a crime for use in a possible criminal prosecution, so long as some residual foreign intelligence purpose of the surveillance also existed.

This simple change of two words masks an underlying dilemma or challenge that permeates FISA and current proposals to amend it,[11] as well as the so-called "NSA surveillance" program,[12] which supporters have called the Terrorist Surveillance Program,[13] conducted without the

[7] *See Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the H. Comm. on the Judiciary*, 107th Cong. 56 (2001).

[8] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (2001).

[9] The 2001 amendment had a five-year limitation. However, it was made permanent in USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 102, 120 Stat. 192, 195 (2006) (to be codified in scattered sections of 18, 50, and other titles of U.S.C.).

[10] 50 U.S.C. § 1804(a)(7)(B) (Supp. I 2003) (emphasis added).

[11] *See* National Security Letter Judicial and Congressional Oversight Act, H.R. 1739, 110th Cong. (2007) (bill to require a FISA judge or designated magistrate to approve national security letters used to share intelligence information among agencies and to require reports that detail these letters' use, including accounts of how "such information has aided such investigations"); NSA Oversight Act, H.R. 11, 110th Cong. (2007) (bill reiterates "that chapters 119 and 121 of title 18, United States Code, and the Foreign Intelligence Surveillance Act of 1978 are the exclusive means by which domestic electronic surveillance may be conducted"); Intelligence Authorization Act for Fiscal Year 2008, H.R. 2082, 110th Cong. (2007) (Sec. 504 makes FISA exclusive means for gathering foreign intelligence information excepting later legislation that purports otherwise); Foreign Intelligence Surveillance Oversight and Resource Enhancement Act of 2007, S. 187, 110th Cong. (2007) (authorizes enhanced congressional oversight over FISA and addresses oversight required for surveillance concerning persons inside the U.S. communicating with persons outside the U.S.); Foreign Intelligence Surveillance Improvement and Enhancement Act of 2007, S. 1114, 110th Cong. (2007) (reiterates FISA is "exclusive means by which electronic surveillance . . . may be conducted" and modernizes surveillance authorities).

[12] *See, e.g.*, James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1. *See also* Press Release, White House, Press Briefing by Attorney General Alberto Gonzales and Principal Deputy Director for National Intelligence (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html.

[13] Alberto Gonzales, Att'y Gen., Prepared Statement of Hon. Alberto R. Gonzales, Attorney General of the United States (Feb. 6, 2006), *available at* http://www.usdoj.gov/ag/speeches/2006/ag_speech_060206.html (explains legality

procedures required by FISA.[14] That dilemma is determining what are the appropriate distinctions to be made, if any, between the procedural and substantive requirements applicable to intrusive searches pursuant to criminal law enforcement investigations and those pursuant to foreign intelligence gathering, including counterintelligence and counterterrorism intelligence gathering. Historically, intelligence surveillances have been subject to less strict requirements than surveillances for law enforcement purposes. Today, with the focus on preventing terrorist acts, especially those with international connections, the tension between law enforcement and intelligence activities has become intense.[15] The legal and historical antecedents of the tension between law enforcement and intelligence searches and surveillances have been explored by a number of commentators[16] and by at least one court,[17] but with all due respect I believe their understandings have contained significant errors. It is the aim of this Article to correct those errors by providing a more accurate historical background that may then serve as an introduction to resolving the dilemma.

II. HISTORY

A. Pre-FISA

It is well established that Presidents have authorized various forms of electronic surveillance for intelligence purposes since at least Franklin

and need for Terrorist Surveillance Program despite program's disregard for FISA provision). *See also* John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON L. REV. 565 (2007) (arguing that Terrorist Surveillance Program is constitutionally based, valid extension of President's wartime power).

[14] While the Administration has agreed to submit the NSA surveillance to the oversight of the Foreign Intelligence Surveillance Court (hereafter "FISC") created by FISA, it has not agreed to abide by the substantive and procedural requirements FISA places on electronic surveillances for foreign intelligence purposes. *See* Letter from Alberto Gonzales, Att'y Gen., to Senators Patrick Leahy and Arlen Specter, (Jan. 17, 2007), *available at* http://www.fas.org/irp/agency/doj/fisa/ag011707.pdf.

[15] For example, Rudy Giuliani, a candidate for the Republican Presidential nomination, has criticized President Clinton for treating the 1993 bomb in the World Trade Center as a criminal act rather than as an act of war. *See, e.g.*, Media Mouse, Giuliani Addresses Crime, Terrorism, and Immigration at Grand Rapids Campaign Stop (June 8, 2007), http://www.mediamouse.org/features/060807giuli.php.

[16] *See, e.g.*, William C. Banks, *The Death of FISA*, 91 MINN. L.REV. 1209 (2007); Diane Carraway Piette & Jesselyn Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall,"* 17 STAN. L. & POL'Y REV. 437 (2006); David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487 (2006); Viet D. Dinh & Wendy J. Keefer, *FISA and the PATRIOT Act: A Look Back and a Look Forward*, 35 GEO. L.J. ANN. REV. CRIM. PROC., at iii (2006); Richard Henry Seamon & William Dylan Gardner, *The PATRIOT Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319 (2005).

[17] *See In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

Roosevelt.[18] Prior to 1967, however, the Supreme Court had held that electronic surveillance by itself was not a "search" under the Fourth Amendment.[19] Consequently, the constitutionality of such surveillance was not seriously questioned. However, a large proportion of the electronic surveillances conducted during this period required a nonconsensual physical entry in order to effectuate the surveillance, and it was assumed by the Federal Bureau of Investigation (FBI) that the Fourth Amendment would require warrants for such physical entries if the surveillance was undertaken for law enforcement purposes.[20] Whether warrants would be required for these physical entries if the purpose was *not* law enforcement was unclear. Moreover, during and after World War II, the FBI engaged in surreptitious physical entries of businesses, homes, and institutions to obtain intelligence information; these entries came to be known as "black bag jobs."[21] Again, it was not clear whether the Fourth Amendment required warrants for these activities.

In *Boyd v. United States*,[22] probably the leading Fourth Amendment case at the time, the Court linked the protection afforded by the Fourth Amendment to protection against use of evidence against a person in a criminal case, saying:

> the "unreasonable searches and seizures" condemned in the fourth amendment are almost always made for the purpose of compelling a man to give evidence against himself, which in criminal cases is condemned in the fifth amendment; and compelling a man "in a criminal case to be a witness against himself," which is condemned in the fifth amendment, throws light on the question as to what is an "unreasonable search and seizure" within the meaning of the

[18] S. REP. NO. 95-604, at 7 (1977) ("[E]very President since Franklin D. Roosevelt asserted the authority to authorize warrantless electronic surveillance and exercised that authority."); *see also* 9/11 COMMISSION REPORT, *supra* note 1, at 74 ("FBI's domestic intelligence gathering dates from the 1930s. With World War II looming, President Franklin D. Roosevelt ordered FBI Director J. Edgar Hoover to investigate foreign and foreign-inspired subversion . . . .")

[19] Olmstead v. United States, 277 U.S. 438, 465 (1928) ("The language of the [Fourth] [A]mendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office, any more than are the highways along which they are stretched.").

[20] *Id.* at 466. (search requires actual physical invasion of house or curtilage, and electronic surveillance not requiring such invasion did not constitute a search).

[21] SENATE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, FINAL REPORT: SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 355 (1976) [hereinafter Church Committee], *available at* http://www.aarclibrary.org/publib/church/reports/book3/html/ChurchB3_0181a.htm (before 1966, FBI conducted two hundred plus "black-bag jobs," another five hundred plus warrantless illegal physical entries for intelligence and nearly as many similar entries for criminal investigatory purposes).

[22] 116 U.S. 616, 633 (1886).

fourth amendment.

In 1959, in *Frank v. Maryland*, the Court, faced with a warrantless search for regulatory purposes, rather than criminal law enforcement, stressed that Fourth Amendment protections were aimed at protecting persons from searches for evidence to be used in criminal trials, saying "history makes plain, that it was on the issue of the right to be secure from searches for evidence to be used in criminal prosecutions or for forfeitures that the great battle for fundamental liberty was fought."[23] Moreover, the Court observed that "[i]nspection without a warrant, as an adjunct to a regulatory scheme for the general welfare of the community and not as a means of enforcing the criminal law, has antecedents deep in our history."[24] Consequently, the Court decided that the Fourth Amendment did not require a warrant for such a regulatory inspection. While there are and were obvious differences between surreptitious physical entries for intelligence purposes and for building code inspections, the doctrinal link between a requirement for a warrant and the use of evidence in a criminal case provided an arguable justification for an exemption from a warrant requirement for intelligence activities not intended to produce evidence for a criminal trial.

While the Fourth Amendment did not impose any obstacles to electronic surveillance, the Communications Act of 1934 did.[25] It made it a crime for any person to "intercept any communication and divulge or publish the . . . contents" of wire and radio communications,[26] and the Supreme Court interpreted this provision to apply to the government and consequently held that evidence so obtained was not admissible in court.[27] Nevertheless, the government interpreted the provision as only prohibiting interception followed by divulging or publishing the contents outside the federal establishment,[28] so that intelligence surveillances could continue.[29]

Thus, early on, there was a legal reason to distinguish FBI operations as being *either* for intelligence *or* for law enforcement. In the former situation, the Fourth Amendment would arguably not require a warrant, whereas in the latter situation a warrant would be required. In addition, if the electronic surveillance of wire or radio communications was not intended to produce evidence for a criminal trial, but merely to be used

[23] Frank v. Maryland, 359 U.S. 360, 365 (1959), *overruled by* Camara v. Mun. Court, 387 U.S. 523 (1967).

[24] *Id.* at 367.

[25] 47 U.S.C. § 605 (1964).

[26] *Id.*

[27] Nardone v. United States, 302 U.S. 379, 380–82 (1937). *See also* Nardone v. United States, 308 U.S. 338, 340 (1939) (extending exclusion to the fruits of the surveillance).

[28] *See* S. REP. NO. 95-604, at 10 (1977).

[29] Of course, the Communications Act provision only related to wire and radio communications, not to listening devices ("bugs").

for intelligence purposes, the government's interpretation of the Communications Act would allow for the warrantless interceptions. Moreover, given the uncertainties in the government's legal conclusion that warrants would not be required for surreptitious entries for intelligence purposes, there was an incentive in not bringing criminal cases that would use information obtained either from such entries or from electronic surveillances that required surreptitious entries. It was better not to test the legal theory unless absolutely necessary.

Beyond the legal issues, there were practical reasons to separate intelligence operations from law enforcement activities. First and foremost, traditionally, intelligence operations are undertaken simply to obtain information on the intentions, capabilities, and activities of those able to harm the United States, information usually unrelated to criminal activity that might be prosecuted, which is why Central Intelligence Agency (CIA) and the military intelligence agencies are not involved in criminal enforcement activities. This is frequently true even with respect to operations directed at activities that usually will at some point become criminal, such as espionage or terrorism. Successful counterintelligence operations often, if not normally, conclude not with prosecution but some other form of neutralization, such as "doubling" an agent.[30] Even counterterrorism operations often involve ongoing infiltration and monitoring as the purpose of the operation, rather than criminal prosecution.[31] Second, there are disincentives to prosecution of targets of counterintelligence and counterterrorism operations. Especially with electronic surveillance, as with undercover spies, it is often important not to reveal ongoing intelligence operations or to disclose "sources and methods." If the object of the surveillance is criminally prosecuted on the basis of information obtained through the surveillance, it is probable, if not certain, that the source of the information would be compromised, thereby destroying its future usefulness.[32] Finally, simple matters of

[30] For example, the FBI arrested Rudolf Abel, a Soviet agent who operated undercover for ten years in New York City, only after failing to "double" him. *See* Abel v. United States, 362 U.S. 217, 223, 226 (1960). *See also* 140 Cong. Rec. 4688, 4701 (1994) (statement of Sen. Cohen) ("Prosecution is one way, but only one way and not always the best way, to combat such activities. 'Doubling' an agent or feeding him false or useless information are other ways. Monitoring him to discover other spies, their tradecraft and equipment can be vitally useful. Prosecution, while disabling one known agent, may only mean that the foreign power replaces him with one whom it may take years to find or who may never be found").

[31] *See* H.R. REP. NO. 95-1283, pt. 1, at 43–44 (1978) ("[Even in cases in which terrorists have violated U.S. law] it may be more fruitful in terms of combating international terrorism to monitor the activities of such persons in the United States to identify otherwise unknown terrorists here, their international support structure, and the location of their weapons or explosives.").

[32] U.S. GEN. ACCOUNTING OFFICE, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED 14–15 (July 2001), [hereinafter GAO Report], *available at* http://fas.org/irp//gao/d01780.pdf (discusses possibility of exposing intelligence sources when

expertise come into play. The skills and strengths of an Elliott Ness are not necessarily valuable in counterintelligence or foreign intelligence operations. Consequently, parallel tracks evolved in the FBI with different career paths.[33] Needless to say, the CIA and military intelligence agencies have no experience, much less expertise, in building criminal cases and think only of intelligence values.

Assuming that warrantless intelligence searches and surveillances could be justified under the Fourth Amendment, such that, if necessary, the information could be used in a criminal prosecution as incidentally acquired information, it was important that the purpose for the surveillance was for intelligence, not law enforcement purposes. This need was highlighted in probably the most famous spy prosecution, that of Colonel Rudolf Abel of the KGB.[34] There, Abel was arrested pursuant to an immigration arrest warrant for the purpose of deportation on the basis of information supplied by the FBI to the Immigration and Naturalization Service (INS) suggesting that Abel was an illegal alien. The arresting INS agents were accompanied by FBI agents, and the FBI agents searched Abel's residence incident to the arrest, looking for and finding evidence of espionage. Abel challenged the lawfulness of the search, arguing that his immigration arrest was simply a ruse to enable the FBI to search his residence. The Court responded:

> Were this claim justified by the record, it would indeed reveal a serious misconduct by law-enforcing officers. The deliberate use by the Government of an administrative warrant for the purpose of gathering evidence in a criminal case must meet stern resistance by the courts. The preliminary stages of a criminal prosecution must be pursued in strict obedience to the safeguards and restrictions of the Constitution and laws of the United States.[35]

While the Court found no evidence of bad faith and upheld the search,[36] the lesson of the case was clear—the FBI could not use non-law enforcement methods for the purpose of gathering evidence for criminal prosecutions.

In short, for various reasons, legal and practical, a "wall," if not "the wall," existed long before FISA.

In 1967, two cases changed the playing field with respect to

government concurrently pursues law enforcement and intelligence ends and conflicts that thus arise as well as the need to balance the competing interests or choose one interest over the other).

[33] *See* 9/11 COMMISSION REPORT, *supra* note 1, at 74.

[34] *See* Abel, 362 U.S. at 218–25. *See also* LOUISE BERNIKOW, ABEL (Ballantine Books 1982) (1970) (biographical account of Abel's life, focusing on his spy work, arrest, trial, and the government's exchanging him for U-2 pilot Gary Powers); Federal Bureau of Investigation, FBI History—Famous Cases: Rudolph Ivanovich Abel (Hollow Nickel Case), http://www.fbi.gov/libref/historic/famcases/abel/abel.htm (overview of Abel's espionage and the FBI's pursuit thereof).

[35] *Abel*, 362 U.S. at 226.

[36] *Id.*

intelligence searches and surveillances. First, *Katz v. United States*[37] overruled *Olmstead v. United States*[38] and declared both that electronic surveillance is a search within the meaning of the Fourth Amendment and that the Fourth Amendment requires a prior warrant to authorize such surveillance. However, the Court included a footnote relevant to intelligence surveillances: "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."[39] First, it is noteworthy that the Court only raised the possibility of a lack of a warrant requirement in national security electronic surveillances, not the possibility that they were not subject to the Fourth Amendment. Second, the Court referred to "national security" surveillances, not surveillances for "intelligence" information, as opposed to evidence of a crime. Thus, it is not clear whether the footnote held open the possibility of a lack of a warrant requirement for "national security" surveillances, even if instituted for criminal law enforcement purposes, or whether the footnote referred only to "national security" surveillances performed for intelligence purposes. However, because the government itself had only represented that it only used such surveillances for intelligence purposes and not for evidentiary purposes,[40] the latter is probably the better understanding.

The second case was *Camara v. Municipal Court*,[41] which overruled *Frank v. Maryland*, rejecting the notion that the need for warrants was occasioned not by the search itself but by the purpose of the search—to obtain evidence for a criminal prosecution. This seriously undercut the argument that the Fourth Amendment would not require warrants for "intelligence" searches simply because they were not intended to obtain evidence for a criminal prosecution.

Nevertheless, the footnote in *Katz* provided a possible opening for "national security" surveillances, and shortly thereafter a provision of Title III of the Omnibus Crime Control and Safe Streets Act[42] reinforced such an opening. That law responded to *Katz* by authorizing electronic

---

[37] 389 U.S. 347 (1967).

[38] 277 U.S. 438 (1928).

[39] *Katz*, 389 U.S. at 358 n.23. The origin of the footnote is not certain; there is no mention of national security in the government's brief. However, the year before *Katz*, the Solicitor General provided a supplemental brief in a case involving surreptitious microphone surveillance in a law enforcement case explaining that historically the FBI had used such devices "for intelligence (and not evidentiary) purposes . . . in the interests of internal security or national safety . . . . Present departmental practice . . . prohibits the use of such listening devices (as well as the interception of telephone and other wire communications) in all instances other than those involving the collection of intelligence affecting the national security." S. REP. NO. 95-604, at 11–12 (1977). This recent revelation must have been on the Court's mind when it decided *Katz*.

[40] *See supra* note 39.

[41] 387 U.S. 523 (1967).

[42] 18 U.S.C. §§ 2510–2520 (Supp. V 1970).

surveillance for obtaining evidence regarding various serious crimes pursuant to a warrant procedure in the law and otherwise criminalizing electronic surveillance by any person.[43] However, it also contained a proviso that mirrored with more specificity the footnote in *Katz*:

> Nothing contained in this chapter or in section 605 of the Communications Act of 1934 . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.[44]

Together, the *Katz* footnote and the Title III proviso could be read to constitute both a Legislative and Judicial ratification of government practice, although neither in fact stated agreement with government practice.

The period immediately following *Katz* and Title III coincides with the most intense opposition to the war in Vietnam and racial disturbances following the assassination of Martin Luther King. As has been amply demonstrated,[45] the government utilized extensive electronic surveillance against opponents of the war and various "Black Power" figures. This led to the *Keith* case[46] in 1972, which involved electronic surveillance conducted for "domestic security" purposes. Here the government was not trying to use any information obtained from the surveillance, but the defendants, having discovered that they had been subject to warrantless electronic surveillance, argued that such surveillance was unconstitutional and demanded a hearing to determine whether any of the evidence to be used against them was the "fruit" of that surveillance. While the government denied that any of its evidence was derived from the surveillance, it wished to avoid a hearing on and disclosure of the facts involving the surveillance. Therefore, it argued

---

[43] *Id.* (Sec. 801 of Pub. L. No. 90-351 explains rationale for law, including need to protect privacy, provide required security tools, and safeguard the integrity of the courts. Sec. 605 sets out illegalities).

[44] 18 U.S.C. § 2511(3) (Supp. V 1970), *repealed by* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 201(c), 92 Stat. 178 (1978).

[45] *See* Church Committee, *supra* note 21, at 185–224, 475–79, 483–89 (covers surveillance of Black Panthers and anti-war demonstrators). *See also* COMM'N ON CIA ACTIVITIES WITHIN THE U.S., REPORT TO THE PRESIDENT 26 (1975) (concludes CIA went beyond acceptable surveillance of various domestic groups).

[46] United States v. U. S. Dist. Ct. (Keith), 407 U.S. 297 (1972) (known as the "Keith" case because the judge of the United States District Court, the respondent in the case, was Judge Damon Keith).

that the surveillance was lawful because it was undertaken to obtain "intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government"[47] and thus within the "national security" exception "recognized" by *Katz* and Title III. The Court quickly dismissed any suggestion that Title III's proviso was intended to or did authorize such a surveillance. The Court stated that "[the proviso] certainly confers no power, as the language is wholly inappropriate for such a purpose. It merely provides that the Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution. In short, Congress simply left presidential powers where it found them."[48] Consequently, the issue was joined—did the President have a constitutional authority to engage in warrantless electronic surveillance for domestic security intelligence purposes? The Supreme Court described the government's argument as claiming that:

> the special circumstances applicable to domestic security surveillances necessitate a further exception to the warrant requirement. . . . We are told further that these surveillances are directed primarily to the collecting and maintaining of intelligence with respect to subversive forces, and are not an attempt to gather evidence for specific criminal prosecutions. It is said that this type of surveillance should not be subject to traditional warrant requirements which were established to govern investigation of criminal activity, not ongoing intelligence gathering.[49]

Nevertheless, weighing the asserted government need against the principles and values protected by the Fourth Amendment, the Court unanimously held that the surveillance was unconstitutional and concluded that prior warrants would be required for such surveillances.[50] Again, however, the Court expressly limited the scope of its decision. "[T]his case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents."[51] And, it included a footnote citing to two lower court cases[52] and an

[47] *Id.* at 300 n.2.

[48] *Id.* at 303.

[49] *Id.* at 318–19.

[50] This opinion was written by Justice Powell, who, perhaps uniquely on the Court, was acquainted with electronic surveillance. *See* JOHN C. JEFFRIES, JR., JUSTICE LEWIS F. POWELL, JR. 92–95 (1994) (during World War II, Powell's primary responsibility was "to evaluate Ultra intelligence, [and] present it in useable form to the Commanding Officer" and to integrate and present various sources of information, "observation, low-level 'Y' radio intercepts, agents and collaborators, prisoners of war, and captured documents").

[51] *See Keith*, 407 U.S. at 321–22.

[52] *See* United States v. Smith, 321 F. Supp. 424, 425–26 (C.D. Cal. 1971); United States v. Clay, 430 F.2d 165 (5th Cir. 1970).

American Bar Association project,[53] all of which held that warrantless surveillance was constitutional "where foreign powers are involved."[54] The loophole had now been narrowed to cases where foreign powers were involved.

Keith was followed by several lower court cases involving surveillance where foreign powers were involved but where the communications of American citizens were overheard.[55] The number of cases and their consistent upholding of warrantless foreign intelligence electronic surveillance was reassuring to the government, but wolves were at the door. The D.C. Circuit in an en banc decision broke ranks with the other circuits that had upheld foreign intelligence surveillances. In *Zweibon v. Mitchell*,[56] the court found a surveillance of the Jewish Defense League (JDL) unconstitutional because, although the JDL was engaged in international terrorist activities, there was no showing that the JDL was itself a foreign power or an agent of a foreign power, and therefore surveillance of it did not fit within the *Keith* exception. Worse, from the government's perspective, a plurality of the court went further and opined in dictum that even if the JDL had been an agent of a foreign power, a warrantless surveillance would have been unconstitutional.[57]

In addition, the publicity surrounding various abuses by intelligence agencies, including NSA surveillance of Americans and drug traffickers, U.S. Army military intelligence surveillance of domestic groups, FBI covert operations against alleged subversive groups, CIA opening of domestic mail sent to or received from abroad, and electronic surveillance of political "enemies," fanned by investigations and reports by the Senate, the House, and the Executive branch had significant effects. First, it fostered congressional attempts to regulate or ban electronic surveillance for intelligence purposes.[58] Second, it undermined the morale and determination of personnel in the intelligence agencies, who viewed such surveillance as a critical tool but who now had some fears that they subsequently would be identified as abusers of civil liberties. Third, private parties whose assistance was often

[53] American Bar Association Project on Standards for Criminal Justice, Electronic Surveillance 120, 121 (Approved Draft 1971 & Feb. 1971 Supp. 11).

[54] *See Keith*, 407 U.S. at 322, n.20.

[55] *See* United States v. Brown, 484 F.2d 418 (5th Cir. 1973) (upheld warrantless wiretap against U.S. citizen); United States v. Butenko, 494 F.2d 593 (3rd Cir. 1974) (wiretap valid if primary purpose to gather foreign intelligence information); United States. v. Buck**,** 548 F.2d 871, 875 (9th Cir. 1977) (warrantless surveillance is "lawful for the purpose of gathering foreign intelligence").

[56] 516 F.2d 594 (D.C. Cir. 1975) (en banc).

[57] *Id.* at 613–14 ("an analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional" (footnote omitted)).

[58] *See* National Security Surveillance Act of 1975, S. 743, 94th Cong. (1975); United States v. Falvey, 540 F. Supp. 1306, 1311 n.12 (E.D.N.Y. 1982) (citing Freedom from Surveillance Act of 1974, S. 4062, 93d Cong. (1974) and Surveillance Practices and Procedures Act of 1973, S. 2820, 93d Cong. (1973).

necessary to performing electronic surveillance were beginning to back away from such assistance. In the past they had thought they were acting in a patriotic manner, but they now saw themselves pilloried as accomplices to illegal action. American Telephone & Telegraph, then still the sole provider of telephone communications in the United States, as well as the limited number of international communications providers, were being sued for assisting the government in identified intelligence operations.[59]

From the Executive branch's perspective, a law authorizing electronic surveillance for foreign intelligence purposes would provide the legal assurance and political affirmation of such surveillance to enable it to continue in appropriate cases. The trick would be to enact a bill that would both enable the intelligence agencies to engage in that surveillance they thought necessary and still pass the gauntlet of civil libertarians, then in ascendance in Congress. There were risks to be run in supporting a bill, because if the civil libertarians had their way, the bill might be unacceptable to the intelligence agencies, and it would be politically costly for the President to veto the bill after initially supporting it. White House Counsel Philip Buchen and Attorney General Edward Levi, nevertheless, supported the idea of going forward with a bill. Secretary of State Henry Kissinger opposed it, arguing in favor of relying upon Presidential authority. President Gerald Ford decided the issue in favor of White House Counsel Buchen and Attorney General Levi, and the administration moved forward toward a bill.

From Congress's perspective, a bill regarding electronic surveillance for foreign intelligence purposes would be beneficial. It would provide evidence that Congress was doing something in reaction to the past abuses that it had uncovered and would protect against possible future executive excesses. Indeed, bills had already been introduced, but absent administration support (or at least acquiescence) they were not likely to pass or be able to overcome a veto. At the same time, among many in Congress, there was a fear that a "political" response to past abuses might indeed jeopardize the ability to obtain needed foreign intelligence. That is, if Congress acted in response to those making the loudest noise, any bill would likely radically restrict the gathering of foreign intelligence.[60]

---

[59] *See Foreign Intelligence Surveillance Act: Hearings on H.R. 7308 Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the H. Comm. on the Judiciary*, 95th Cong. 64–65 (1978) (Hon. Morgan F. Murphy testifying that FISA legislation would make the phone company "feel much more secure" in complying with electronic surveillance requests); *see also S. 2726 to Improve U.S. Counterintelligence Measures: Hearings on S. 2726 Before the S. Select Comm. on Intelligence*, 101st Cong. 136 (1990) (testimony of Mary Lawton, Counsel, Office of Intelligence Policy and Review, U.S. Department of Justice) (noting the failure of the phone company to cooperate with electronic surveillance requests).

[60] For example, the American Civil Liberties Union seriously proposed banning the use of electronic surveillance altogether. *See Foreign Intelligence Surveillance Act of 1976: Hearing on S. 743, S. 1888 & S. 3197 Before the Subcomm. on Criminal Laws and*

B. FISA

Whether it was Senator Edward Kennedy who first approached Attorney General Levi, or vice versa, is not clear, but it was their initial agreement to find a middle path, a pragmatic path, that enabled FISA to become a reality. A collaborative enterprise involving both Senator Kennedy's assistant, Kenneth Feinberg, and staff of the Attorney General, produced a draft bill that Senator Kennedy introduced as S. 3197 in 1976.[61] The bill first underwent hearings in the Senate Judiciary Committee[62] and, as amended, was reported out by that committee.[63] It was also considered by the Senate Intelligence Committee,[64] which also reported it out with amendments,[65] but the session ran out before the bill could be considered by the full Senate. It was also considered by the House Judiciary Committee,[66] but no further action was taken in the House. In the next Congress, Senator Kennedy again introduced the bill as it had been last reported.[67] The administration had changed, but the Carter administration also supported the bill. Again, the Senate acted first, with both the Senate Judiciary Committee and the Senate Intelligence Committee holding hearings[68] and then reporting the bill,[69] and the Senate passed it on April 20, 1978. In the House, the House Intelligence Committee held hearings[70] and then reported the bill to the floor,[71] where it passed on September 7, 1978. A conference committee was convened, which reported a conference bill that was agreed to by the

Procedures of the Comm. on the Judiciary, 94th Cong. 27–37 (1976) (testimony of Morton H. Halperin and John Shattuck of the American Civil Liberties Union).

[61] Foreign Intelligence Surveillance Act of 1976, S. 3197, 94th Cong. (1976).

[62] *Foreign Intelligence Surveillance Act of 1976, supra* note 60.

[63] S. REP. NO. 94-1035, at 1 (1976).

[64] *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings on S. 3197 Before the Subcomm. on Intelligence and the Rights of Americans of the S. Comm. on Intelligence*, 94th Cong. (1976)

[65] S. REP. NO. 94-1161, at 1–2 (1976).

[66] *Foreign Intelligence Surveillance Act: Hearings Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the H. Comm. on the Judiciary*, 94th Cong. (1976).

[67] S. 1566, 95th Cong. (1977). In the House the bill was H.R. 7308, 95th Cong. (1977).

[68] *See Foreign Intelligence Surveillance Act of 1977: Hearings on S. 1566 Before the Subcomm. on Criminal Laws and Procedures of the S. Comm. on the Judiciary*, 95th Cong. (1977); *Foreign Intelligence Surveillance Act of 1978: Hearing on S. 1566 Before the Subcomm. on Intelligence and the Rights of Americans of the S. Select Comm. on Intelligence,* 95th Cong. (1978).

[69] *See* S. REP. NO. 95-604, at 1 (1977); FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, S. REP. NO. 95-701, at 1 (1978).

[70] *See Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308 & H.R. 5632 Before the Subcomm. on Legis. of the H. Select Comm. on Intelligence*, 95th Cong. (1978).

[71] *See* H.R. REP. NO. 95-1283, pt. 1, at 1 (1978).

Senate on October 9 and by the House on October 12, 1978.[72] On October 25, 1978, the President signed the Foreign Intelligence Surveillance Act, and it became law.

As passed, FISA authorized "electronic surveillance"[73] of a "foreign power"[74] or "agent of a foreign power"[75] to obtain "foreign intelligence

[72] *See* H.R. REP. NO. 95-1720 (1978) (Conf. Rep.).

[73] "Electronic surveillance" was defined to include four different forms of surveillance. *See* 50 U.S.C. § 1801(f) (1982). It included the acquisition in the United States of a "wire communication" (a communication *while* being carried by wire) from a person in the United States, § 1801(f)(2); the acquisition of a wire or radio communication by targeting a known "United States person" who is in the United States, if a warrant would be required for law enforcement purposes, § 1801(f)(1); the intentional acquisition of a radio communication between or among persons located in the United States if a warrant would be required for law enforcement purposes, § 1801(f)(3); and the installation or use of a device for monitoring to acquire information other than from a wire or radio communication if a warrant would be required for law enforcement purposes, § 1801(f)(4). The first of these would include ordinary wiretaps, and the last would include ordinary "bugging." The second and third would include various radio communications (e.g., cell phone transmissions, microwave transmissions, and satellite transmissions, as well as CB, ham, and other radio communications). Together they were intended to cover all electronic surveillance in the United States directed at persons in the United States. It was not intended to cover surveillances abroad or even surveillances of communications to the United States if conducted abroad. *See, e.g.*, H.R. REP. NO. 95-1283, pt. 1, at 50–51.

[74] "Foreign power" was defined to include two separate sets of entities. *See* 50 U.S.C. § 1801(a). The first set included foreign governments, factions of foreign nations, and entities acknowledged to be controlled by a foreign government or governments. § 1801(a)(1)–(3). The second set included groups engaged in international terrorism, foreign-based political organizations, and entities directed or controlled by a foreign government or governments. § 1801(a)(4)–(6). The distinction was that the former were clearly and openly "foreign," so that United States persons would not be members, whereas the latter, while "foreign," were more likely to have United States persons as members or employees.

[75] "Agent of a foreign power" was defined differently depending upon whether the person was a "United States person." *See infra* note 78; 50 U.S.C. § 1801(b). If the person was not a United States person, any officer, employee, or member of a "foreign power" qualified as an "agent of a foreign power." § 1801(b)(1)(A). In addition, if the person was not a United States person, a person would qualify as an "agent of a foreign power" if the person acted on behalf of a foreign power that engaged in clandestine intelligence activities in the United States and the circumstances indicated the person might engage in such activities. § 1801(b)(1)(B). Finally, if the person was not a United States person, the person qualified as an "agent of a foreign power" if the person aided, abetted, or conspired with any person to engage in clandestine intelligence activities. *Id.* If the person *was* a United States person, the person would qualify as an "agent of a foreign power" if on behalf of a foreign power the person knowingly engaged in sabotage, international terrorism, or clandestine intelligence activities, which activities "involve or may involve" a violation of the criminal laws of the United States, § 1801(b)(2)(A)–(C), or if the person knowingly aided, abetted, or conspired with any person engaged in those activities, § 1801(b)(2)(D). Thus, in order for a United States person to be an "agent of a foreign power," the person would have to be involved in one of the described activities in a manner that either was a violation of law or might involve a violation of

information"[76] under two separate regimes. If the Attorney General certified under oath that the surveillance was solely directed at the communications transmitted exclusively between certain "foreign powers"[77] and the surveillance was one that was not intended to and was unlikely to obtain the communications of a "United States person,"[78] the Attorney General could authorize the surveillance himself for a period of up to one year.[79] In all other circumstances, however, FISA required a court order to authorize the surveillance.[80] In order to obtain such an order, the Attorney General had to submit an application to the Foreign Intelligence Surveillance Court (FISC)[81] that contains certain information and certifications.[82] The information required included: the identity or a description of the target of the surveillance, the facts and circumstances justifying the belief that the target is a foreign power or agent of a foreign power and that the place at which the surveillance is directed is being used or about to be used by a foreign power or agent of a foreign power, the means by which the surveillance will be effected and whether physical entry will be used, the proposed "minimization procedures,"[83] and a description of the information sought and the type

law at some time. This differed from the standards under Title III of the Omnibus Crime Control and Safe Streets Act, which requires a showing of probable cause that the target of the surveillance "is committing, has committed, or is about to commit" an offense specified in the Act and that "particular communications concerning that offense will be obtained," 18 U.S.C. § 2518(3)(a)–(b), by allowing surveillance of United States persons when their activities only "may involve" specified criminal violations.

[76] "Foreign intelligence information" was defined in two ways, one describing positive foreign intelligence—information necessary to the national defense or security of the United States or to the conduct of the foreign affairs of the United States—and the other describing counterintelligence, counter-sabotage, and counter-terrorism intelligence—information necessary to protect against attack or other grave hostile acts, sabotage or international terrorism, or clandestine intelligence activities of a foreign power or agent of a foreign power. 50 U.S.C. § 1801(e).

[77] Only surveillances of "foreign powers" within the first set of defined "foreign powers," *see supra* text accompanying note 74, could qualify for Attorney General-authorized surveillances.

[78] "United States person" was defined to include citizens and permanent resident aliens, organizations substantially comprising such persons, and corporations incorporated in the United States that did not qualify as a "foreign power" included in the first set of "foreign powers." 50 U.S.C. § 1801(i).

[79] 50 U.S.C. § 1802(a)(1) (1982).

[80] 50 U.S.C. § 1802(b).

[81] 50 U.S.C. § 1803 (1982). The title, "Foreign Intelligence Surveillance Court" does not appear in FISA. This section also created a court of review to which the government could take appeals if the FISC denied an application. This court is named the Foreign Intelligence Surveillance Court of Review.

[82] 50 U.S.C. § 1804(a) (1982).

[83] "Minimization procedures" were defined to mean specific procedures adopted by the Attorney General to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons" consistent with intelligence needs, but which allow for the retention

of communications or activities subject to the surveillance.[84] There were three certifications required to be made by a high executive official[85]: that the purpose of the surveillance is to obtain foreign intelligence information, that the information sought is foreign intelligence information (including a designation of what kind of foreign intelligence information it is and an explanation of the basis for this designation), and that the information cannot reasonably be obtained through normal means (including a statement explaining why this is so).[86] A judge of the Foreign Intelligence Surveillance Court then could issue an order authorizing the surveillance for up to ninety days[87] if the judge found that the proposed minimization procedures met the statutory definition,[88] the application contained the required certifications (and, if the target of the surveillance was a United States person, that the certification was not clearly erroneous),[89] and that there was probable cause to believe that the target was a foreign power or agent of a foreign power and that the place at which the surveillance was directed is being used or about to be used by a foreign power or agent of a foreign power.[90]

As originally introduced, the bill's first operative provision provided that under FISA a judge could approve electronic surveillance of a foreign power or agent of a foreign power "*for the purpose of obtaining foreign intelligence information.*"[91] Despite a multitude of changes to the bill over two Congresses and three congressional committees, that original language never changed.[92] Indeed, even today that language remains unchanged in current law.[93] The first congressional committee to consider the bill added a requirement that the application for an order include a certification that "the purpose of the surveillance is to obtain foreign intelligence information"[94] and that the judge find that the certification is present and, if the surveillance is of a United States

and dissemination for law enforcement purposes of information that is evidence of a crime. 50 U.S.C. § 1801(h).

[84] 50 U.S.C. § 1804(a)(3)–(6), (8).

[85] The certifications could be made by the Assistant to the President for National Security Affairs or an official designated by the President from those appointed by the President with the advice and consent of the Senate. 50 U.S.C. § 1804(a)(7).

[86] 50 U.S.C. § 1804(a)(7).

[87] 50 U.S.C. § 1805(d)(1) (1982).

[88] 50 U.S.C. § 1805(a)(4).

[89] 50 U.S.C. § 1805(a)(5).

[90] 50 U.S.C. § 1805(a)(3).

[91] *Foreign Intelligence Surveillance Act: Hearing on H.R. 12750 Before the Subcomm. on Courts, Civil Liberties and the Administration of Justice of the H. Comm. on the Judiciary*, 94th Cong. 3 (1976) (text of H.R. 12750) (emphasis added).

[92] 50 U.S.C. § 1802(b) (1982). When FISA was amended in 1994 to add a chapter on physical searches, identical language was included there. 50 U.S.C. § 1822(b) (1994).

[93] *See* 50 U.S.C. § 1802(b) (2000).

[94] *See* 50 U.S.C. § 1804(a)(7)(B) (1982).

person,[95] that the certification is not clearly erroneous.[96] The explanation for the addition was:

> This requirement is designed to prevent the practice of targeting one individual for electronic surveillance when the true purpose of the surveillance is to gather information about another individual. It is also designed to *make explicit that the sole purpose of such surveillance is to secure foreign intelligence information and not to obtain information for any other purpose.*[97]

The requirement for this certification and the judicial review of it remained unchanged thereafter throughout the legislative process, and each subsequent committee report repeated verbatim the explanation for the provision.[98]

It is clear that this language was never intended to preclude the dissemination and use of foreign intelligence information for law enforcement purposes, so long as the purpose of the surveillance was to acquire foreign intelligence information. For example, Senate Bill 3197, as reported by the Senate Judiciary Committee in 1976, the same bill in which the purpose requirement first appeared, specifically provided in its provision on the "Use of Information" that:

> (a) Information acquired from an electronic surveillance . . . may be used by and disclosed . . . only for purposes relating to the ability of the United States to protect itself against actual or potential attack or other hostile acts of a foreign power or its agents; to provide for the security or national defense of the Nation or the conduct of foreign affairs of the United States; or to protect the national security against foreign intelligence activities *or for the enforcement of the criminal law.*[99]

The report language explained this provision as limiting the "lawful uses of foreign intelligence information" to "actual foreign intelligence purposes and the enforcement of the criminal law."[100] Similar, if not identical, language also appears in the subsequent committee reports.[101]

What is notable about this language is that it distinguishes between the use of foreign intelligence information for foreign intelligence purposes and for law enforcement purposes. This is not surprising given the background to the legislative initiative. If the government intended

---

[95] *See* 50 U.S.C. § 1801(i) (1982) (definition of "United States person").

[96] *See* S. REP. NO. 94-1035, at 2, 3, 19, 36, 39, 61, 62 (1976).

[97] *Id.* at 36 (emphasis added).

[98] *See* S. REP. NO. 94-1161, at 33 (1976) (regarding S. 3197); S. REP. NO. 95-604, at 12 (1977) (regarding S. 1566); S. REP. NO. 95-701 (1978); H.R. REP. NO. 95-1283, pt. 1, at 76 (1978) (regarding H.R. 7308). When FISA was amended in 1994 to add a chapter dealing with physical searches, an identical certification requirement was included. *See* 50 U.S.C. §§ 1823(a)(7)(B), 1824(a)(5) (1994).

[99] S. REP. NO. 94-1035, at 64 (emphasis added).

[100] *Id.* at 43.

[101] *See* S. REP. NO. 94-1161, at 39; S. REP. NO. 95-604, at 39, 46; S. REP. NO. 95-701, at 41, 59; H.R. REP. NO. 95-1283, pt. 1, at 87.

to obtain evidence for prosecution of espionage, sabotage, as well as a broad array of other criminal statutes that might be violated by spies or terrorists, Title III had always provided a means for obtaining warrants for electronic surveillance.[102] FISA was deemed unnecessary for that. It was precisely when the purpose of the surveillance was *not* law enforcement that no statute authorized the surveillance. The government's arguments for the constitutionality of warrantless electronic surveillance for foreign intelligence purposes had always relied on the fact that the purpose was not law enforcement but intelligence gathering,[103] and the case law upholding such warrantless surveillance had accepted the government's argument and likewise had stressed that the purpose was to obtain foreign intelligence.[104] The administration's desire for legislation was for a statutory procedure authorizing what the administration had been doing previously without a warrant or statutory authorization—electronic surveillance for the purpose of obtaining foreign intelligence, not for the purpose of prosecuting criminal offenses.[105] Moreover, in arguing in support of the legislation, the

[102] 18 U.S.C. § 2516(1) (1976).

[103] *See, e.g.*, United States v. Butenko, 494 F.2d 593, 601 (3d Cir. 1974) ("The Attorney General has certified . . . that the surveillances at issue here 'were conducted and maintained solely for the purpose of gathering foreign intelligence information'"); Zweibon v. Mitchell, 516 F.2d 594, 608 n.23 (D.C. Cir. 1975) ("Although we accept . . . appellees' assertion that the purpose of the surveillance was intelligence gathering, these and other aspects of the facts before us demonstrate the potential for abuse of such surveillance as a means for circumventing the warrant requirement in normal criminal investigations." (citations omitted)); United States v. Smith, 321 F. Supp. 424, 428 (C.D. Cal. 1971) ("The government has emphasized that the purpose of the surveillance involved was 'not to gather evidence for use in a criminal prosecution but rather to provide intelligence information needed to protect against the illegal attacks of such organizations.'"). *See also* S. REP. NO. 95-604, at 11 (quoting from a brief of the Solicitor General to the Supreme Court in the case of Black v. United States, 385 U.S. 26 (1966): "Under departmental practice in effect for a period of years prior to 1963, and continuing until 1965, the Director of the [FBI] was given authority to approve the installation of [electronic surveillance] devices . . . for intelligence (and not evidentiary) purposes. . . . Present departmental practice . . . prohibits the use of [electronic surveillance] devices . . . in all instances other than those involving the collection of intelligence affecting the national security.").

[104] *See, e.g.*, United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973) ("the President may constitutionally authorize warrantless wiretaps for the purpose of gathering foreign intelligence"); *Butenko*, 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."). *See also* United States v. Truong Dinh Hung, 629 F.2d 908, 915–16 (4th Cir. 1980) (holding that in order to be constitutional a warrantless surveillance must be "primarily" for foreign intelligence, not law enforcement, purposes); *Zweibon* 516 F.2d at 694 (Wilkey, J., concurring in part and dissenting in part).

[105] *See* Exec. Order No. 12,036, 3 C.F.R. 100 (1978) ("Activities described in sections 2-202 through 2-205 for which a warrant would be required if undertaken for law enforcement rather than intelligence purposes shall not be undertaken against a

government repeatedly stressed that the purpose of the legislation was not law enforcement but foreign intelligence gathering,[106] a position consistent with what it represented in court cases.[107]

This understanding was clearly shared by Congress. The first bill introduced proposed to create a new chapter in the United States Code entitled "Electronic Surveillance Within the United States For Foreign Intelligence Purposes,"[108] and it continues to be the given title of Title I of FISA.[109] The committee reports on this and the subsequent bills likewise reflected this understanding, repeatedly stating that the legislation is to authorize electronic surveillance "for foreign intelligence purposes."[110] The particular distinction between surveillances for foreign

United States person without a judicial warrant, unless the President has authorized the type of activity involved and the Attorney General has both approved the particular activity and determined that there is probable cause to believe that the United States person is an agent of a foreign power."), revoked by Exec. Order No. 12,333, 46 Fed. Reg. 59,951 (Dec. 4, 1981) ("The Attorney General hereby is delegated the power to approve the use for intelligence purposes, within the United States or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is probable cause to believe that the technique is directed against a foreign power or an agent of a foreign power.").

[106] *See, e.g.*, *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearings on S. 3197 Before the Subcomm. on Intelligence and the Rights of Americans of the S. Select Comm. on Intelligence*, 94th Cong. 76–77 (1976) (testimony of Attorney General Edward Levi).

[107] *See* United States v. Humphrey, 456 F. Supp. 51, 56 (E.D. Va. 1978) ("If the [government] representations . . . can be credited, it is rare that foreign intelligence surveillance is undertaken with plans to prosecute."), *aff'd sub nom.* United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

[108] Foreign Intelligence Surveillance Act of 1976, S. 3197, 94th Cong. (1976).

[109] *See* 50 U.S.C. § 1804 (1982).

[110] *See, e.g.*, S. REP. NO. 95-604, at 5 (1977) ("The purpose of the bill is to provide a procedure under which the Attorney General can obtain a judicial warrant authorizing the use of electronic surveillance in the United States *for foreign intelligence purposes*."); *id.* ("S. 1566 authorizes the Chief Justice of the United States to designate seven district court judges, any one of whom may hear applications for and grant orders approving electronic surveillance *for foreign intelligence purposes*."); *id.* at 7 ("The Federal Government has never enacted legislation to regulate the use of electronic surveillance within the United States *for foreign intelligence purposes*."); *id.* at 15 ("This legislation would provide the secure framework by which the Executive Branch may conduct legitimate electronic surveillance *for foreign intelligence purposes* within the context of this Nation's commitment to privacy and individual rights."); *id.* at 16 ("The basis for this legislation is the understanding—concurred in by the Attorney General—that even if the President has an 'inherent' constitutional power to authorize warrantless surveillance *for foreign intelligence purposes*, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance."); *id.* at 47 ("Subsection (a) of this section is patterned after 18 U.S.C. Section 2518(3) and specifies the findings the judge must make before he grants an order approving the use of electronic surveillance *for foreign intelligence purposes*."); *id.* at 50 ("In the Committee's view 90 days is the maximum length of time during which a surveillance of these persons or

intelligence purposes and for law enforcement purposes is strikingly evident in the definitions of "electronic surveillance."[111] There, three of the four different definitions define electronic surveillance for purposes of FISA in terms of circumstances when "a warrant would be required for law enforcement purposes,"[112] and the fourth definition did not require that language because it was believed that in those circumstances a warrant was always required for law enforcement purposes.[113] Thus, a surveillance for foreign intelligence purposes, as opposed to law enforcement purposes, would require a FISA warrant if a warrant would be required for "law enforcement purposes," clearly suggesting that a FISA surveillance was not "for law enforcement purposes."

This distinction between surveillances for foreign intelligence purposes and for law enforcement purposes was further noted by Congress in the discussion of the minimization requirements in the bills,

entities *for foreign intelligence purposes* should continue without new judicial scrutiny.") (emphases added)); H.R. REP. NO. 95-1283, pt. 1, at 21 ("[One of the reasons why there is a need for this legislation is that] the development of standards and restrictions by the judiciary with respect to electronic surveillance *for foreign intelligence purposes* accomplished through case law threatens both civil liberties and the national security . . . ."); *id.* ("While oversight can be . . . an important adjunct to control of intelligence activities, it cannot substitute for public laws, publicly debated and adopted, which specify under what circumstances and under what restrictions electronics surveillance *for foreign intelligence purposes* can be conducted."); *id.* at 22 ("The purpose of the bill is to provide a statutory procedure authorizing the use of electronic surveillance in the United States *for foreign intelligence purposes*. The procedures in the bill would be the exclusive means by which electronic surveillance, as defined, could be used *for foreign intelligence purposes*."); *id.* at 23 ("The bill would require a prior judicial warrant for all electronic surveillance *for foreign intelligence purposes* with three limited exceptions."); *id.* at 24 ("The purpose of the Foreign Intelligence Surveillance Act is to provide legislative authorization for and regulation of all electronic surveillance conducted within the United States *for foreign intelligence purposes*."); *id.* ("Thus, even if the President has the inherent authority in the absence of legislation to authorize warrantless electronic surveillance *for foreign intelligence purposes*, Congress has the power to regulate the conduct of such surveillance by legislating a reasonable procedure."); *id.* at 24–25 ("A basic premise behind this bill is the presumption that whenever an electronic surveillance *for foreign intelligence purposes* may involve the fourth amendment rights of any U.S. person, approval for such a surveillance should come from a neutral and impartial magistrate."); *id.* at 27 ("[K]nowledgeable officials in the intelligence agencies have earnestly suggested to the committee that this bill will further our national security by facilitating the electronic surveillance necessary *for foreign intelligence purposes*."); *id.* at 28 ("Title I of the Foreign Intelligence Surveillance Act contains the substantive provisions governing the conduct of electronic surveillance *for foreign intelligence purposes*."); *id.* at 68 ("Subsection (a) of this section authorizes the President, acting through the Attorney General, to approve electronic surveillances *for foreign intelligence purposes* without a judicial warrant in certain circumstances.") (emphases added).

[111] 50 U.S.C. § 1801(f) (1982).

[112] 50 U.S.C. § 1801(f)(1), (3), (4).

[113] 50 U.S.C. § 1801(f)(2) (intercepting in the United States wire communications to or from a person in the United States without either party's consent).

justifying the different minimization requirements under the bills from those in Title III[114] in light of the different purposes of the surveillances.[115] Another example is in commentary on the procedures applicable to use of FISA-obtained information in criminal prosecutions.[116] In describing this provision, which was contained in the original bill, the Senate Judiciary Committee stated:

> Although the primary purpose of electronic surveillance conducted pursuant to this chapter will not be the gathering of criminal evidence, it is contemplated that such evidence may occasionally be acquired and this subsection and the succeeding one establish the procedural mechanisms by which such information may be used in judicial proceedings.[117]

Identical or virtually identical language appears in each of the succeeding committee reports.[118] The members likewise believed that the purpose of the bill was to gather intelligence, not evidence.[119] Indeed, whereas the Senate committees had included FISA in a new chapter directly following the chapter on law enforcement electronic surveillance in Title 18 of the United States Code, which pertains to the criminal law, the House committee rejected that approach. It stated:

> In the committee's view, the placement of [FISA] in title 18 would be misleading. Nothing in [FISA] relates to law enforcement procedures . . . . Placing [FISA] in title 18 would wrongly suggest either that the bill's procedures deal with law enforcement or that the thrust of the bill is to create a Federal crime. Because the bill instead establishes authorities and procedures dealing with the collection of foreign intelligence, the committee believes that its proper placement would be in title 50 (War and National Defense), United States Code. Title 50 has traditionally been the title in which laws relating to this Nation's intelligence activities have been placed.[120]

After both Senate committee reports were issued and after the House Intelligence Committee hearings, an important espionage case was decided by a court in the northern district of Virginia, the *Truong*

---

[114] *See* 18 U.S.C. § 2518 (5) (1994).

[115] *See* S. REP. NO. 94-1161, at 39 (1976); S. REP. NO. 94-1035, at 38–39 (1976); S. REP. NO. 95-604, at 39 (1977); S. REP. NO. 95-701, at 14, 41–42 (1978); H.R. REP. NO. 95-1283, pt. 1, at 60 (1978).

[116] *See* 50 U.S.C. § 1804 (2000).

[117] S. REP. NO. 94-1035, at 44.

[118] *See* S. REP. NO. 94-1161, at 41; S. REP. NO. 95-604, at 55; S. REP. NO. 95-701, at 62; H.R. REP. NO. 95-1283, pt. 1, at 89.

[119] *See, e.g.*, H.R.. REP. NO. 95-1283, at 118 (Remarks of Mr. McClory: "the government does not seek the information to prosecute. While prosecution may prove to be a viable option, the main thrust of our efforts in this area are [sic] to protect against foreign intelligence activities which threaten our security. Prosecution may be, as most often has been the case, inappropriate or harmful to that effort.").

[120] H.R. Rep. No. 95-1283, pt. 1, at 28.

decision.[121] In *Truong*, the FBI initiated a warrantless electronic surveillance of Truong, who was passing classified State Department information to representatives of the Vietnamese government for the purpose of obtaining foreign intelligence.[122] However, at some point during the surveillance, the purpose changed from intelligence to law enforcement, and the decision to prosecute Truong was made. At trial, Truong argued that the warrantless surveillance was unconstitutional and moved to suppress all evidence derived from the surveillance. The court held that the surveillance was constitutional when it was initiated, following the case law finding an exception to the warrant requirement for foreign intelligence surveillances authorized by the President.[123] However, the court went on to decide that when the primary purpose of the surveillance changed from intelligence gathering to law enforcement, a warrant was required.[124] Consequently, the court suppressed evidence derived from the surveillance after the date upon which the court decided the primary purpose had become law enforcement.[125]

On its face, the *Truong* district court decision did not relate to FISA's requirements. To the contrary, the court held that *absent a warrant* the primary purpose of a surveillance must be to obtain foreign intelligence information. Obviously, as under Title III, with a warrant the primary purpose of a surveillance could be law enforcement. Whether the "warrant" authorized by FISA, under laxer strictures than under Title III, would be constitutional if it purported to authorize surveillances for law enforcement purposes was not before the court and was not addressed by the court. When *Truong* was appealed, the court of appeals affirmed the decision of the court below and agreed with the lower court's primary purpose requirement for warrantless surveillances, as well as its factual determinations that initially the surveillance was for the primary purpose of obtaining foreign intelligence information but that later the primary purpose became law enforcement.[126] In a footnote, the court of appeals noted the passage of FISA since the decision below.[127] The court explained why, despite the apparent ability to have a warrant requirement for certain foreign intelligence surveillance, the court would not find a constitutional requirement for a warrant, saying "the complexity of [FISA] also suggests that the imposition of a warrant requirement, beyond the constitutional minimum described in this opinion, should be left to the intricate balancing performed in the

[121] United States v. Humphrey, 456 F. Supp. 51 (E.D. Va. 1978), *aff'd sub nom.* United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

[122] *Humphrey*, 456 F. Supp. at 54; *Truong*, 629 F.2d at 911–12.

[123] *Id.* at 57.

[124] *Id.* at 57–59.

[125] *Id.* at 59.

[126] *Truong*, 629 F.2d at 915–16.

[127] *Id.* at 914 n.4.

course of the legislative process by Congress and the President."[128] Because the court thereafter described the primary purpose test as constitutionally required,[129] some have read this to suggest that a primary purpose test was constitutionally required in FISA.[130] In context this seems unlikely, as the *Truong* court goes out of its way to stress how courts should defer to a Legislative/Executive compromise in this area,[131] and as the Foreign Intelligence Surveillance Review Court noted much later, the *Truong* court "had no occasion to consider the application of the statute carefully."[132]

The district court opinion in *Truong* appeared after both Senate committees had reported S. 1566 and after the House committee's hearings. The Committee did, however, become aware of it.[133] Nevertheless, there is no mention of the case in the committee report itself, and apparently no attempt to address the implications of the case.[134] Why that might be is unknown, but one plausible reason is that

[128] *Id.*

[129] *Id.* at 915–16.

[130] *See, e.g.*, *In re* Sealed Case, 310 F.3d 717, 742 (FISA Ct. Rev. 2002).

[131] *See Truong* 629 F.2d at 914 n.4 ("The elaborate structure of the statute demonstrates that the political branches need great flexibility to reach the compromises and formulate the standards which will govern foreign intelligence surveillance. Thus, the Act teaches that it would be unwise for the judiciary, inexpert in foreign intelligence, to attempt to enunciate an equally elaborate structure for core foreign intelligence surveillance under the guise of a constitutional decision.").

[132] *In re Sealed Case*, 310 F.3d at 742.

[133] *See* H.R. REP. NO. 95-1283, pt. 1, at 109, 114 (1978) (additional views of Representatives Morgan F. Murphy and Charles Rose, stating that there was a civil suit brought against the Attorney General arising out of that portion of the *Truong* surveillance that had been declared unconstitutional; dissenting views on H.R. 7308, noting that every court had upheld the constitutionality of warrantless electronic surveillance for foreign intelligence gathering and citing *Truong*).

[134] There was one addition to the House Report pertaining to the definition of "foreign intelligence information." The report pointed out that the definition included information necessary to the ability of the United States to protect against sabotage, terrorism, and clandestine intelligence activities. Moreover, the report noted that "foreign intelligence information" might well include information that also would be evidence of a crime. It then stated:

> How this information may be used "to protect" against clandestine intelligence activities is not prescribed by the definition of foreign intelligence information . . . . Obviously, use of "foreign intelligence information" as evidence in a criminal trial is one way the Government can lawfully protect against clandestine intelligence activities, sabotage, and international terrorism. The bill, therefore, explicitly recognizes that information which is evidence of crimes involving clandestine intelligence activities, sabotage, and international terrorism can be sought, retained, and used pursuant to this bill.

H.R. REP. NO. 95-1283, pt. 1, at 49. If this explanation was intended to rebut any "primary purpose" requirement in the bill's language requiring that "the purpose" of the surveillance be to "obtain foreign intelligence information," it is less than pellucid. This explanation could be read as easily to mean simply that evidence of a crime gathered in a surveillance undertaken for foreign intelligence purposes is not precluded from being used as evidence in a prosecution. This would be consistent

the primary purpose test the *Truong* court devised for warrantless surveillances was entirely consistent with "the purpose" requirement contained in FISA.

This history leaves the clear impression that the FISA bills were not intended to act as a substitute for Title III warrants when the government wished to engage in surveillance of espionage, sabotage, or terrorism for the purpose of law enforcement, even though there was no restriction on the use of evidence acquired pursuant to a surveillance that was being conducted for foreign intelligence purposes.

C. Post-FISA

In the cases that followed the passage of FISA, in which the government did intend to use the fruits of a FISA surveillance in a criminal prosecution, a routine challenge seeking suppression of the evidence was that the surveillance had not been primarily for foreign intelligence purposes but for law enforcement purposes. This raised two possible questions: did FISA require a primary purpose of obtaining foreign intelligence rather than enforcing the criminal law, and if so, did the surveillance in question have the requisite purpose? Every court to rule on whether FISA contained a primary purpose requirement held that it did.[135] Many courts simply assumed such a requirement, probably because the government did not contest the issue,[136] while some courts

with other language in this and previous reports. Had the intent of this explanation been to rebut a "primary purpose" test, language referencing such a purpose test or the *Truong* case would have been much clearer. Indeed, elsewhere in the report, the Committee addressed "the purpose" of surveillances under the bill, saying, "this committee recognizes full well that the surveillance under this bill are [sic] not primarily for the purpose of gathering evidence of a crime." H.R. REP. NO. 95-1283, pt. 1, at 36.

[135] *See* United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1992); United States v. Pelton, 835 F.2d 1067, 1075–76 (4th Cir. 1987); United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984). *See also* United States v. Ning Wen, 477 F.3d 896, 897 (7th Cir. 2007) (dictum). *But see In re Sealed Case*, 310 F.3d at 727 (dictum) (this decision was not made in the context of a suppression motion). *United States v. Falvey*, 540 F. Supp. 1306 (E.D.N.Y. 1982), is sometimes cited as allowing a FISA surveillance so long as obtaining foreign intelligence is "a" purpose, *see, e.g.*, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978: THE FIRST FIVE YEARS, S. REP. NO. 98-660, at 12 (1984) (quoting a Department of Justice communication), but that is not an accurate statement of the case. In *Falvey* the defendant sought suppression in part on the ground that the purpose of the surveillance was law enforcement, not obtaining foreign intelligence. The court noted that *Truong* had required suppression of a *warrantless* surveillance when the primary purpose was law enforcement, but the court emphasized that in this case there was a warrant, so any evidence obtained pursuant to a lawful FISA warrant would be admissible. Here, the court said, "Defendants argue that the order was not properly issued, because from its inception this was a criminal investigation. To the contrary, I find that the order was properly issued, because the application clearly sought foreign intelligence information." 540 F. Supp. at 1314 n.17.

[136] *See, e.g.*, United States v. Sattar, No. 02 CR. 395 JGK, 2003 WL 22137012, at *12

found it unnecessary to decide the issue, but in *every* case the courts decided that the primary purpose of the surveillance was to obtain foreign intelligence information, not to obtain evidence of a crime.[137] Some of these courts, while not expressly holding that there was a requirement for a primary purpose to obtain foreign intelligence information, did hold that it would be inconsistent with FISA if the sole purpose was to obtain evidence of criminal conduct.[138]

In short, the government interpreted FISA to require the surveillance to have "the purpose" of obtaining foreign intelligence, which meant in practice "the primary purpose" to obtain foreign intelligence. And, in challenges to admission of evidence from FISA surveillances, every court to consider the issue agreed with that interpretation, and no court disagreed with it.[139]

Within the Department of Justice, the Office of Intelligence Policy and Review (OIPR) was the principal office for overseeing the intelligence activities of the Department, and it was the office that actually submitted applications to the Foreign Intelligence Surveillance Court.[140] The primary purpose test as initially interpreted by OIPR allowed the intelligence offices in the FBI to coordinate and communicate with the Criminal Division in the Department of Justice, so long as the Criminal Division did not direct or control the surveillance.[141] This arrangement continued for over fifteen years and appeared to satisfy all parties.[142] However, the combination of a new head of OIPR and

(S.D.N.Y. Sept. 15, 2003) (noting that the Government acknowledged that it had adhered to a primary purpose standard).

[137] *See* United States v. Hammoud, 381 F.3d 316, 334 (4th Cir. 2004), *vacated on other grounds*, 543 U.S. 1097 (2005) (avoiding question whether a primary purpose is required); *Johnson*, 952 F.2d at 572 (finding primary purpose required); United States v. Sarkissian, 841 F.2d 959, 964 (9th Cir. 1988) (explicitly declining to decide whether there is a primary purpose requirement); *Pelton*, 835 F.2d at 1075–76 (finding a primary purpose required); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987) (apparently assuming a primary purpose requirement); *Duggan*, 743 F.2d at 77 (finding primary purpose required); *Falvey*, 540 F. Supp. at 1314 (apparently assuming a primary purpose standard).

[138] *See, e.g.*, *Sarkissian*, 841 F.2d at 964 (stating that the purpose of the surveillance must be to secure foreign intelligence information and citing to *United States v. Cavanagh*, 807 F.2d 787, 790-91 (9th Cir. 1987) for the proposition that the purpose of the surveillance is "not to ferret out criminal activity but rather to gather intelligence"). *See also In re Sealed Case*, 310 F.3d at 735 (holding that FISA as amended by the USA PATRIOT Act precludes having the sole purpose of criminal enforcement—"if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct—even foreign intelligence crimes—to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied"); *accord Sattar*, 2003 WL 22137012, at *10.

[139] *But see In re Sealed Case*, 310 F.3d at 727 (stating in dictum that FISA did not impose a primary purpose test).

[140] *See* 9/11 COMMISSION REPORT, *supra* note 1, at 78.

[141] *Id.*; BELLOWS REPORT, *supra* note 4, at 711–12.

[142] *See* BELLOWS REPORT, *supra* note 4, at 711–12. *See also* Americo R. Cinquegrana,

concerns related to the Aldrich Ames case seems to have changed the situation in 1994.[143] Aldrich Ames was a CIA employee who was transmitting classified information to the Soviet Union and later to the Russian Foreign Intelligence Service, and beginning in 1993 the FBI subjected Ames to extensive surveillance pursuant to FISA orders.[144] Upon Ames' arrest in 1994, the new head of OIPR was concerned that "because of the numerous prior consultations between FBI agents and prosecutors, the judge might rule that the FISA warrants had been misused."[145] Why that might be so is unclear. The original investigation was a classic counterintelligence investigation—to confirm Ames was a spy, to identify his contacts, to discover his tradecraft, and to monitor his activities. His actual arrest was occasioned by his planning an official trip to Russia, where it was feared he would defect. That is, the case looks very similar to some other cases in which courts ruled that the primary purpose of the surveillance was to obtain foreign intelligence, not to enforce the criminal law.[146] Moreover, the sheer number of previous cases over the years in which courts had found the requisite primary purpose despite the relatively free coordination between the FBI and the Criminal Division should have provided some sense of security. In addition, FISA did not permit either the FISC or courts in suppression hearings to second-guess the certification that the purpose of the surveillance was to obtain foreign intelligence information. If the surveillance was directed at United States persons, the FISC was only permitted to assess whether the certification was clearly erroneous,[147] which was the same standard

The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978, 137 U. PA. L. REV. 793, 819, 823–27 (1989) (article by Deputy Counsel for Intelligence Policy in OIPR concerning issues raised by FISA and amendments that might be made nowhere suggests the "primary purpose" test is a problem). However, the Senate Intelligence Committee's five-year report on the implementation of FISA recognized that the Justice Department considered the "primary purpose" test as an issue. *See* THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978: THE FIRST FIVE YEARS, S. REP. NO. 98-660, at 12 (1984). The Committee, however, was not equivocal on the issue: "The Committee believes 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." *Id.* at 15. *See also id.* at 12 ("A renewal application may note the possibility of proceeding to prosecution and explain why, despite this possibility, the continuing foreign intelligence purpose and value of the information sought justifies continued use of FISA rather than Title III procedures.").

[143] *See* BELLOWS REPORT, *supra* note 4, at 711–12; 9/11 COMMISSION REPORT, *supra* note 1, at 78.

[144] *See* Federal Bureau of Investigation, FBI History—Famous Cases: Aldrich Hazen Ames, http://www.fbi.gov/libref/historic/famcases/ames/ames.htm.

[145] *See* 9/11 COMMISSION REPORT, *supra* note 1, at 78.

[146] *See, e.g.*, United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987); United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

[147] *See* 50 U.S.C. § 1805(a)(5) (1982).

governing courts in suppression hearings.[148] OIPR's fears were not tested, as Ames did not go to trial, but instead pleaded guilty to espionage with a sentence of life imprisonment without opportunity for parole, apparently in exchange for a light sentence for his wife, who had aided and abetted his activities.[149]

In any case, the new head of OIPR instituted new rules regarding interactions between FBI intelligence personnel and the Criminal Division that ultimately had the effect of essentially cutting off all communications without the prior approval of OIPR, going well beyond FISA issues.[150] This was the real "wall" that was later to receive such devastating criticism. It was neither compelled nor suggested by the primary purpose test in FISA. The FBI and Justice had complied with FISA for years without such restrictions on coordination and with no court raising any complaint. Moreover, such restrictions on coordination were inconsistent with FISA itself and its legislative history, which repeatedly referenced the possibility of criminal prosecutions and the fact that often foreign intelligence information would itself constitute evidence of a crime.[151] Undoubtedly, FISA presumed that the coordination between intelligence offices and the Criminal Division that had existed before FISA, when warrantless intelligence surveillances clearly could not be for law enforcement purposes, would continue under the new statutorily authorized system. In short, "the wall" constructed by OIPR was not justified under FISA.[152] Indeed, none of the interpretations by the Office of Legal Counsel and intra-departmental reviews supported the OIPR interpretation.[153] It is ironic that the major criticism of the FBI's performance in the Ames case, in a review by the

[148] *See* United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984) ("a reviewing court is to have no greater authority to second-guess the executive branch's certifications than has the FISA judge"). *See also* H.R. REP. NO. 95-1283, pt. 1, at 92–93 ("when reviewing the certifications required by section 104(a)(7), unless there is a prima facie showing of a fraudulent statement by a certifying officer, procedural regularity is the only determination to be made if a non-U.S. person is the target, and the 'clearly erroneous' standard is to be used where a U.S. person is targeted.").

[149] *See* Federal Bureau of Investigation, *supra* note 144.

[150] *See* 9/11 COMMISSION REPORT, *supra* note 1, at 78–79; BELLOWS REPORT, *supra* note 4, at 711–34.

[151] *See, e.g.*, S. REP. NO. 94-1035, at 44 (1976); S. REP. NO. 94-1161, at 41 (1976); S. REP. NO. 95-604, at 55 (1977); S. REP. NO. 95-701, at 10–11, 62 (1978); H.R. REP. NO. 95-1283, pt. 1, at 49, 89 (1978).

[152] Construction of "the wall" was not the only action OIPR took that frustrated the use of FISA. In addition, OIPR took what some thought was an overly strict interpretation of the "probable cause" requirement in FISA. *See, e.g.*, S. REP. NO. 106-352, at 4 (2000). This led to amendments in FISA in 2000 to "clarify and make explicit" what was believed to have been the original intent. *Id. See* Counterintelligence Reform Act of 2000, Pub. L. No. 106-567, §§ 601–604, 114 Stat. 2831, 2850–53, (codified as amended at 50 U.S.C. §§ 1801, 1804, 1808, 1823, 1824 (2000)).

[153] *See* BELLOWS REPORT, *supra* note 4, at 720, 734–52; 9/11 COMMISSION REPORT, *supra* note 1, at 79.

Inspector General of the Department of Justice, was that there had been a lack of coordination and information sharing within the FBI, not that there had been too much coordination.[154]

Unfortunately, OIPR was not the only entity to misconstrue FISA. At some point, the FISC itself seemed to adopt OIPR's interpretation of the need for "the wall."[155] Some have suggested that this was due to the Deputy Counsel of OIPR becoming the Legal Advisor to the FISC.[156] However, it should also be noted that the Presiding Judge of the FISC at that time was Judge Royce Lamberth, a judge who has generated substantial controversy for his hard-ball tactics with government personnel and offices that he believes have misled him.[157] Indeed, he censured a highly regarded FBI agent for misleading the court regarding compliance with "the wall," which the court had imported into the minimization procedures for FISA surveillances.[158] For example, contrary to "the wall's" requirements, in one investigation of a terrorist organization, FBI agents from the criminal investigation acted jointly with FBI agents from the intelligence investigation.[159] As a result, the FISC imposed even more stringent restrictions on the dissemination of surveillance information.[160] Then, it was 9/11.

By September 19, the administration was circulating a draft legislative proposal that included amendments to FISA to eliminate the primary purpose test by deleting the word "the" and replacing it with the word "a" before the word "purpose" with respect to both electronic surveillances and physical searches.[161] The draft section-by-section analysis prepared by the Department of Justice explained the provision.

---

[154] *See* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S PERFORMANCE IN UNCOVERING THE ESPIONAGE ACTIVITIES OF ALDRICH HAZEN AMES (April 1997), *available at* http://www.usdoj.gov/oig/special/9704.htm.

[155] *See In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (FISA Ct. 2002) [hereinafter *In re* All Matters], *rev'd sub nom. In re* Sealed Case, 310 F.3d 717, 721 (FISA Ct. Rev. 2002).

[156] *See* Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, S. REP. NO. 107-351, H.R. REP. NO. 107-792, at 89 n.112 (2002) (additional views of Senator Richard C. Shelby).

[157] *See generally* Stephanie Mencimer, *Lone-Star Justice*, WASH. MONTHLY, April 1 2002. *See also* Richard J. Pierce, Jr., *Judge Lamberth's Reign of Terror at the Department of Interior*, 56 ADMIN. L. REV. 235 (2004).

[158] *See* Memorandum from Judge Royce Lamberth to Attorney General John Ashcroft (Mar. 9, 2001), *available at* http://www.cooperativeresearch.org/sourcedocuments/2001/pdfs/fisacourt20010309.pdf. *See also* OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION PRIOR TO THE SEPTEMBER 11 ATTACKS, at Chapter 2.III.B. (2004), *available at* http://www.usdoj.gov/oig/special/0506/index.htm.

[159] *See id.* at Chapter 2.III.B.1.

[160] *Id.*

[161] *See* The Mobilization Against Terrorism Act (MATA) of 2001, § 153, *available at* http://www.eff.org/Censorship/Terrorism_militias/20010919_mata_bill_draft.html.

> Current law requires that FISA be used only where foreign intelligence gathering is the sole or primary purpose of the investigation. This section will clarify that the certification of a FISA request is supportable where foreign intelligence gathering is "a" purpose of the investigation. This change would eliminate the current need continually to evaluate the relative weight of criminal and intelligence purposes, and would facilitate information sharing between law enforcement and foreign intelligence authorities which is critical to the success of anti-terrorism efforts.[162]

Hearings were held in the House and Senate, and the purpose of the proposed change was described primarily as facilitating the sharing of foreign intelligence information with law enforcement authorities, clearly but not explicitly addressing the then existing problem with the FISC's minimization procedures.[163] While there was some sympathy expressed with regard to the administration's position, several members of the Senate expressed concern about the constitutionality of FISA if the primary purpose test were eliminated.[164] In the Senate this proposal was described as "[t]he most controversial change" proposed by the administration.[165] Senator Feinstein had suggested in the Judiciary Committee hearing to insert the word "significant" after "a" and before

---

[162] *Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the H. Comm. on the Judiciary,* 107th Cong. 56–57 (2001).

[163] *See id.* at 35 (remarks of Assistant Attorney General Chertoff):

> It is wonderful to collect information. But if we can't make use of it, it is a colossal waste of time. One of the critical cornerstones of this legislation is designed to make an amendment in the language of the Foreign Intelligence Surveillance Act that we believe restores the original intent, that allows us to use court-ordered electronic surveillance to get information on potential terrorists, people who are agents of a foreign power, and make sure it gets communicated in a timely fashion to those criminal justice authorities who can arrest people and incapacitate them so that they are no longer out on the street, available to plant a bomb or hijack a plane.
>
> Unfortunately, the way the courts have interpreted the law up to now, they have made it very difficult to bridge that gap. And we've been in the unenviable position of sometimes having intelligence information in the possession of the FBI that the law appears to prohibit them from sharing with the people who would go out and make the case and make the arrest and incapacitate these people.
>
> That is why section 153 of this legislation is critically important. It restores what I think is the original intent of the law, to make sure that there is adequate protection, court protection against surveillance, but a reasonable sharing of information.

Id. Assistant Attorney General Chertoff refers to "courts" interpreting the law in a way making it hard to share FISA obtained information with criminal justice authorities. Undoubtedly, he is referring only to the FISC, which was the only court to have raised any problem with such sharing.

[164] *See, e.g.*, *S. 1448, the Intelligence to Prevent Terrorism Act of 2001 and Legislative Proposals in the Wake of the September 11, 2001 Attacks: Hearings on S.1448 Before the S. Select Comm. on Intelligence,* 107th Cong. 29, 32–33, 36–37 (2001) (remarks of Sens. Feinstein, Dewine, and Edwards).

[165] 147 CONG. REC. S10558 (daily ed. Oct. 11, 2001) (statement of Sen. Leahy).

"purpose."[166] The Department of Justice, in order to alleviate most of the concerns that had been raised, provided a legal opinion that so drafted the bill would be constitutional, and accordingly that change was made to the bill.[167] Senator Leahy further noted that he had proposed, and the administration had accepted, an additional provision to the bill that would clarify "the boundaries for consultation and coordination" between foreign intelligence and law enforcement officials.[168] This provision, amending section 106 of FISA governing the use of information, in effect would dismantle "the wall." It provided:

> (1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against [attacks by a foreign power, sabotage, international terrorism, or espionage].
>
> (2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) or the entry of an order under section 105.[169]

Both this provision and the "significant purpose" provision passed the House and Senate without further amendment.

The "significant purpose" amendment to FISA would seem to have eliminated any question relating to the ability to utilize FISA for law enforcement purposes, so long as some significant foreign intelligence purpose were present.[170] As Senator Leahy stated in describing the amendment: "The Administration's aim was to allow FISA surveillance and search for law enforcement purposes, so long as there was at least some element of a foreign intelligence purpose."[171] As enacted, that element had to be significant. The primary purpose test had been statutorily eliminated.[172] Similarly, the new section 106(k) authorizing consultation with law enforcement officers "to coordinate efforts" likewise seemed to be a clear authorization to tear down "the wall."

---

[166] *Id.*

[167] *Id.*

[168] *Id.*

[169] S. 1510, 107th Cong. § 505 (2001); H.R. 3162, 107th Cong. § 504 (2001).

[170] Unfortunately with regard to clarity, the amendments did not address § 102(b) of FISA, 50 U.S.C. § 1802(b) (1982), which continues to provide that a judge may approve electronic surveillance "for the purpose of obtaining foreign intelligence information." Similarly, they did not address the comparable provision of FISA dealing with physical searches. *See* 50 U.S.C. § 1822(c) (1994). Nevertheless, in light of the legislative history behind the change to § 104(a)(7)(B), 50 U.S.C. § 1804(a)(7)(B), and the mandatory requirement for a judge to issue an order under § 105, 50 U.S.C. § 1805, if all the requirements there are met, there seems little legal force to "the purpose" language in § 102(b).

[171] 147 CONG. REC. at S10558.

[172] While the USA PATRIOT Act's provisions were only temporary, they have now been made permanent. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 102, 120 Stat. 192, 195 (2006).

The FISC, however, did not see it that way. In light of the amendments to FISA, in March 2002, the Department of Justice altered its internal procedures and submitted a motion to the FISC to amend the minimization procedures the court had imposed on FISA surveillances, which had been adopted to institutionalize "the wall." The FISC denied the motion. In an opinion rendered by Judge Lamberth, but signed by all seven judges of the court, the court stated that "the collection of foreign intelligence information is the *raison d'etre* for the FISA," and accordingly the court's "jurisdiction is limited to granting orders for electronic surveillances and physical searches for the collection of foreign intelligence information. . . ."[173] The court then denied that its decision was based on an interpretation of its jurisdiction,[174] and it explicitly declined to address whether FISA could be used primarily for law enforcement purposes.[175] Rather, the court said, its decision was based on its interpretation of the statute's minimization procedures requirement.[176] The court acknowledged that the proposed new minimization procedures were designed to regulate the dissemination of information, consultation, and provision of advice between intelligence and law enforcement officials, and that they would supersede the prior internal procedures that had been incorporated by the FISC into the minimization procedures. The court described at some length its use of the Department of Justice's internal procedures, "the wall," a term used by the court itself, as minimization procedures "[i]n order to preserve both the appearance and the fact that FISA surveillances and searches were not being used *sub rosa* for criminal investigations . . . ."[177] The court noted the history of violations of "the wall," its referral of the matter to the Department of Justice, and the failure of the Department of Justice, after more than a year, to complete a report on the matter.[178] The court then described the new proposed procedures that would allow dissemination of FISA material to criminal prosecutors, extensive consultation between law enforcement and intelligence officials, and worst of all (from the FISC's perspective) the ability of criminal

[173] *In re* All Matters, 218 F. Supp. 2d 611, 613-14 (FISA Ct. 2002).

[174] *See Id.* at 614 n.1.

[175] *Id.* at 615 n.2.

[176] *Id.*

[177] *Id.* at 620.

[178] The tone of the opinion, harshly criticizing unauthorized dissemination and sharing of FISA information with FBI law enforcement personnel, reads like prime Judge Lamberth. *See* Cobell v. Norton, 226 F. Supp. 2d 1 (D.D.C. 2002), *vacated*, 334 F.3d 1128 (D.C. Cir. 2003). *See also* Cobell v. Kempthorne, 455 F.3d 317, 335 (D.C. Cir. 2006) (removing Judge Lamberth from the case: "[R]easonable observers must have confidence that judicial decisions flow from the impartial application of law to fact, not from a judge's animosity toward a party—we conclude, reluctantly, that this is one of those rare cases in which reassignment is necessary."). That the Department of Justice in the months following 9/11 may have had higher priorities than making a report to Judge Lamberth on past minimization violations apparently did not occur to the FISC.

prosecutors to "advise *FBI intelligence officials* concerning '*the initiation, operation, continuation, or expansion of FISA searches or surveillance.*'"[179] These procedures, the court said, were "designed to enhance the acquisition, retention and dissemination of *evidence for law enforcement purposes, instead* of being consistent with the need of the United States to 'obtain, produce, and disseminate *foreign intelligence information.*'"[180] Moreover, the court noted that the new proposed procedures would eliminate the prohibition in the prior wall procedures prohibiting criminal prosecutors from directing or controlling FISA cases. For these reasons, the court found the new procedures in violation of the FISA requirements for minimization.

Despite its protestations to the contrary, the FISC seemed clearly to reject any effect of the amendment to FISA changing "the purpose" of the surveillance to obtain foreign intelligence information to only "a significant purpose" of the surveillance. The court ignored the legislative history of the provision expressing the intent that surveillances could be undertaken for law enforcement purposes, at least as long as there remained some significant foreign intelligence purpose. Moreover, the court nowhere acknowledged the amendment to FISA specifically authorizing intelligence officers to consult with law enforcement officers to coordinate efforts.[181] Thus, it is not surprising that on appeal the Foreign Intelligence Surveillance Review Court reversed the FISC's decision.[182] What is surprising is the method by which the Review Court reached its decision.

The Review Court, rather than directly assessing the validity of the FISC's decision under the amended FISA, proceeded first to ask whether under FISA, as enacted in 1978, the FISC could have imposed the restrictions of "the wall" that it had. It concluded that FISC's restrictions were invalid even under the original FISA, because in the court's view the original FISA did not contain a primary purpose requirement.[183] This, despite the almost 4,000 words expended, however, is all dictum—the holding of the court is clear: "we conclude that FISA, *as amended by the Patriot Act*, supports the government's position, and that the restrictions imposed by the FISA court are not required by FISA or the Constitution."[184] The Review Court relied on the language and legislative history of the amendments as described above to reach the unremarkable conclusion that the FISC's restrictions were unauthorized.

---

[179] *In re All Matters*, 218 F. Supp. 2d at 622–23.

[180] *Id.* at 623.

[181] *See* 50 U.S.C. § 1806(k) (2000 & Supp. 2001).

[182] *See In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002).

[183] The Review Court is thus the only court ever to conclude that "the purpose" requirement of FISA did not require a "primary purpose" of obtaining foreign intelligence information. This Article has earlier concluded that indeed the primary purpose interpretation that had been shared by all concerned was correct.

[184] *Id.* at 719–20 (emphasis added, footnote omitted).

Nevertheless, it is important to consider the Review Court's analysis of the original FISA, because it has, at least in part, been accepted by some commentators[185] and has been cited by the Department of Justice before other courts.[186] The Review Court believed that the primary purpose test had been invented by the *Truong* appellate court,[187] whose opinion was delivered after the passage of FISA and therefore could not have been incorporated into FISA. As discussed at some length above, however, the primary purpose test, predated *Truong* and had long been the government's own understanding of what was required for warrantless surveillances. And, it was those surveillances for which the administration sought to obtain authorization in FISA. The government was not seeking an expanded scope beyond the traditional foreign intelligence surveillances, and Congress certainly did not intend to provide *greater* scope to the government's surveillances than it had exercised in the past. The Review Court ignored or was not aware of the significant legislative history supporting a primary purpose requirement,[188] and it minimized the post-FISA case law finding a primary purpose requirement because those cases did not "tie[] the 'primary purpose' test to *actual* statutory language."[189] The Review Court also ignored totally the arguments contained in the FISC's opinion for why it believed there had been a primary purpose test. Finally, the Review Court was not persuaded by the fact that both the government in seeking the amendments to FISA and Congress in enacting them had proceeded upon the understanding that FISA originally did contain a primary purpose requirement.[190]

Instead, the Review Court accepted the government's argument, which the court recognized "ha[d] never previously been advanced either before a court or Congress."[191] The essence of that argument was

---

[185] *See* Seamon & Gardner, *supra* note 16.

[186] *See, e.g.*, United States v. Hammoud, 381 F.3d 316, 333-34 (4th Cir. 2004). Inasmuch as the Review Court's proceeding was an ex parte proceeding, *see In re Sealed Case*, 310 F.3d at 721 n.6, one should question the precedential value of the opinion in other traditional cases. The fact that the Review Court allowed the American Civil Liberties Union and the National Association of Criminal Defense Lawyers to file briefs as amici curiae should not change the essential nature of the ex parte proceeding.

[187] *See In re Sealed Case*, 310 F.3d at 725.

[188] The Review Court only acknowledged one statement, which it characterized as an "observation, not a proscription." *Id.*

[189] *Id.* at 726. In quoting from one case, however, the Review Court deleted from the quotation the citation to actual FISA provisions that the court had made. *See* United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984).

[190] *See In re Sealed Case*, 310 F.3d at 734–36.

[191] *Id.* at 721. In fact, this argument had been mentioned to Congress during hearings on the USA PATRIOT Act. *See S. 1448, the Intelligence to Prevent Terrorism Act of 2001 and Legislative Proposals in the Wake of the September 11, 2001 Attacks*, *supra* note 164 (remarks of Associate Deputy Attorney General Kris). Associate Deputy Attorney General Kris, after discussing the primary purpose test and how it had been

that section 104(a)(7)(B) in the original FISA stated that "the purpose" of the *surveillance* was to obtain "foreign intelligence information"; it did not state or limit what the purpose was or how that information might be used, so long as it was "foreign intelligence information." In other words, the purpose requirement did not bar the government from having at the time of seeking the FISA order the primary purpose to use the foreign intelligence information obtained from the surveillance for criminal prosecution purposes. Because the defined term, "foreign intelligence information," included "information that relates to and . . . is necessary to . . . the ability of the United States to protect against . . . grave hostile acts of a foreign power or agent of a foreign power; or sabotage or international terrorism by a foreign power or agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power," the government could truthfully certify that it had the purpose of obtaining foreign intelligence information if it had the sole purpose of obtaining evidence of violations of criminal law necessary to prosecute, for example, terrorists. That evidence would be "foreign intelligence information" because the use of such information to prosecute someone would enable "the United States to protect against . . . international terrorism. . . ."

This argument is not without some merit if one only read the certification requirement and the definition of foreign intelligence information in isolation from the rest of FISA and its legislative history. Moreover, some legislative history can be read to support this interpretation,[192] although for the most part that history can also be read simply to make clear that there was no limitation on the use of FISA material for prosecution of foreign intelligence crimes when the surveillance was undertaken for foreign intelligence purposes. However, as described in detail above, the origins of FISA and other legislative history are directly at odds with such an interpretation. Moreover, it is at

interpreted, offered, "Now there is an argument. . . ." Upon concluding the description of the argument, he stated, "But that argument would be, I think, new." *Id.* at 33.

[192] *See, e.g.*, H.R. REP. NO. 95-1283, pt. 1, at 49 (1978) ("the term 'foreign intelligence information' . . . can include evidence of certain crimes relating to sabotage, international terrorism, or clandestine intelligence activities. . . . [F]oreign intelligence information includes information necessary to protect against [these kinds of activities]. . . . Obviously, use of 'foreign intelligence information' as evidence in a criminal trial is one way the Government can lawfully protect against [these kinds of activities]. The bill, therefore, explicitly recognizes that information which is evidence of crimes involving [these kinds of activities] can be sought, retained, and used pursuant to this bill."); S. REP. NO. 95-701, at 10–11 (1978) ("U.S. persons may be authorized targets, and the surveillance is part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnapping, and terrorist acts committed by or on behalf of foreign powers. Intelligence and criminal law enforcement tend to merge in this area. . . . [S]urveillances conducted under [FISA] need not stop once conclusive evidence of a crime is obtained, but instead may be extended longer where protective measures other than arrest and prosecution are more appropriate.").

odds with the consistent interpretation by the government and the courts until *In re Sealed Case*. Finally, as the Review Court acknowledged, Congress's action in amending FISA as requested by the government is at odds with such an interpretation.[193] In assessing today the correct interpretation of FISA as enacted, the understandings of the government over the years before FISA's amendment, the interpretations of several courts, and the explicit understanding of the Congress amending FISA are relevant. In any case, the Review Court concluded that this argument could no longer be used with respect to FISA as amended.[194] It specifically held that the government could not base a surveillance solely on the need to "gain evidence of past criminal conduct—even foreign intelligence crimes—to punish the agent rather than halt ongoing espionage or terrorist activity."[195] Moreover, the court rejected the government's claim that surveillances to obtain evidence of non-foreign intelligence crimes in order to prosecute suspected terrorists, for example, would be authorized because such prosecutions would neutralize those persons, thereby protecting against future terrorism.[196] That, the court said, went beyond even the original FISA, because the legislative history was clear that one of the purposes of "the purpose" requirement was to prohibit targeting a person where the purpose was not to obtain foreign intelligence information.[197]

As already noted, the Review Court's conclusion that FISA as originally enacted did not contain a primary purpose requirement was

[193] *In re Sealed Case*, 310 F.3d at 734–36. Moreover, it was also inconsistent with the interpretation evidenced by the Senate Select Committee on Intelligence in its five-year review of the operation of FISA. *See* S. REP. NO. 98-660, at 15 (1984) ("The Committee believes 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.").

[194] *In re Sealed Case*, 310 F.3d at 735. As I understand them, Seamon and Gardner (*supra* note 16) part from the Review Court here.

[195] *In re Sealed Case*, 310 F.3d at 735. The court may mean that surveillance would not be authorized because the information sought would not "protect against" future foreign intelligence crimes and, therefore, would not be "foreign intelligence information," or that the surveillance would not be authorized because the sole purpose would be prosecution, leaving no residual significant foreign intelligence purpose.

[196] *Id.* at 735–36.

[197] *Id.* at 736. This seems inconsistent with court's analysis of the original FISA. After all, if "foreign intelligence information" includes any information that could protect the United States against terrorism and locking up a terrorist for income tax violations would incapacitate him, thereby protecting the United States from his terrorist activities, then information enabling such a prosecution would seem to meet the definition of "foreign intelligence information." I believe the logic behind the government's claim here further indicates the invalidity of its basic argument to the Review Court that the original FISA authorized surveillances that had the primary (even sole) purpose of obtaining evidence to be used in court against agents of foreign powers.

pure dictum because of its independent conclusion that the USA PATRIOT Act created "a significant purpose" requirement, which was inconsistent with the FISC's minimization procedures. At this point, however, the Review Court was faced with the constitutional question: would surveillance pursuant to FISA's procedures remain constitutional[198] if that surveillance was conducted primarily for law enforcement purposes with respect to a foreign intelligence crime? The Review Court found that FISA was still constitutional.[199] While the court was not willing to hold that a FISA "order" constituted a "warrant" under the Fourth Amendment,[200] it "firmly" believed that surveillances authorized by FISA as amended would be "reasonable" under the Fourth Amendment.[201] In reaching this conclusion, the court thoughtfully considered the *Truong* opinion, but concluded that *Truong*'s "primary purpose" test was intended to be a constitutional requirement only when the surveillance occurred under the warrantless, Attorney General-authorized surveillances at issue in that case.[202] In addition, the court compared the requirements of Title III and FISA and found that "in many significant respects the two statutes are equivalent."[203] Nevertheless, the court allowed that the two statutes "diverge[d] in constitutionally relevant areas—in particular, in their probable cause and particularity showings."[204] This fact, however, does not by itself suggest unconstitutionality, because no court has held that all the particulars of Title III are constitutionally required, and because the Supreme Court in *Keith* clearly suggested that even domestic security surveillances might be authorized on a less protective standard than Title III.[205] The Review Court also considered recent Supreme Court cases involving "special needs" searches[206]—other searches that do not require traditional

[198] Prior to FISA's amendment, numerous courts upheld the constitutionality of the warrant procedure under FISA against attacks under the Fourth Amendment. *See, e.g.*, United States v. Duggan, 743 F.2d 59 (2d Cir. 1984). No judge on any court found it unconstitutional.

[199] *See In re Sealed Case*, 310 F.3d at 746.

[200] *Id.* ("[W]e think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close."). Other courts, however, have found that the original FISA order constituted a Fourth Amendment warrant, and as such was constitutional. *See, e.g.*, United States v. Cavanagh, 807 F.2d 787, 790 (9th Cir. 1987).

[201] *In re Sealed Case*, 310 F.3d at 746.

[202] *Id.* at 742–44.

[203] *Id.* at 741.

[204] *Id.*

[205] *See* United States v. U.S. Dist. Ct. (Keith), 407 U.S. 297, 322 (1972) ("[W]e do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.'").

[206] *See In re Sealed Case*, 310 F.3d at 745–46.

probable cause—but apparently did not find much there to assist it.[207] Ultimately, in light of the similarities between Title III orders and FISA orders, and the *Keith* Court's suggestion of an allowance for domestic security searches, the Review Court believed FISA surveillances would meet the reasonableness of the Fourth Amendment, despite the lack of a primary purpose test.

With one exception, subsequent cases have cited *In re Sealed Case* for the proposition that FISA surveillances are constitutional, [208] but they have done so without any analysis or recognition that *In re Sealed Case* was issued in an ex parte proceeding, or even recognition that FISA was amended in perhaps a constitutionally significant manner in the USA PATRIOT Act.[209] This is not to suggest that the Review Court was necessarily wrong on the issue before it. The constitutional issue before the court was whether FISA as amended was facially unconstitutional. Its conclusion, which it conceded was not governed by any "definitive jurisprudential answer,"[210] is highly defensible. The real test, however, should be at least in a traditional adversarial proceeding and preferably in an as-applied case. Therefore it is disappointing that subsequent courts in this situation have not recognized these distinctions in their analyses. Nevertheless, in *Mayfield v. United States*,[211] a district court found in a facial challenge[212] that the "significant purpose" amendment rendered FISA unconstitutional. The court rejected the Review Court's analysis and held that the Fourth Amendment requires a traditional warrant when the purpose of the search or surveillance is to gather evidence for use in a criminal prosecution. The government is appealing this case, and it will likely be decided sometime in late 2008.

III. REFLECTIONS

The above history is intended to demonstrate that the so-called "primary purpose" test was implicit in FISA's "the purpose" requirement for certifications made to the FISC. It was implicit because the government only conceived that it would seek surveillances under FISA if the primary purpose was to obtain foreign intelligence, and the government only conceived that it would seek such surveillances, because those were the only surveillances it had sought under Presidential/Attorney General authorization, and it was only those

[207] *Id.* at 746.

[208] *See, e.g.*, United States v. Damrah, 412 F.3d 618, 625 (6th Cir. 2005).

[209] *Id.* In *Damrah*, for example, the court cites to pre-USA PATRIOT Act cases for the proposition that courts have uniformly found FISA constitutional.

[210] *In re Sealed Case*, 310 F.3d at 746.

[211] 504 F. Supp. 2d 1023 (D. Or. 2007).

[212] The court explicitly states that it is deciding a facial challenge, *see* 504 F. Supp. 2d at 1035–36, but part of its analysis relies on the alleged fact that the surveillance in question was done for law enforcement purposes, *see* 504 F. Supp. 2d at 1038.

surveillances that were sought to be authorized by FISA.

Inasmuch as this limitation was implicit in the nature of the surveillances the government sought to have authorized by FISA, this limitation was not enacted in response to identified past or imagined future abuses. That is, there is no legislative history suggesting a concern with abusive surveillances undertaken specifically to obtain evidence of crimes relating to foreign intelligence or terrorist activities. Thus, the requirement that "the purpose" of surveillances be to obtain "foreign intelligence information" was not enacted to avoid perceived abuses involved in enforcing criminal laws against espionage, sabotage, and terrorism with respect to agents of foreign powers pursuant to FISA. Only in the legislative history of the FISA amendments do we see for the first time a congressional expression of concern about using FISA surveillances specifically for law enforcement purposes.[213] And here the concern is whether FISA surveillances for law enforcement purposes would be constitutional because they could be used primarily for law enforcement purposes, *an issue that had never arisen in the consideration of the original FISA*. Clearly, had the original FISA ever been considered to provide for surveillances for law enforcement purposes, the same constitutional considerations would have been raised at that time. This provides further evidence that it was not within the contemplation of the government or Congress that the original FISA could be used primarily for law enforcement purposes. Nevertheless, the fact that "the purpose" limitation arose not from a congressional desire to foreclose abuses but from a limit on what the government sought to obtain through FISA should not change the legal conclusion that the limitation existed.

The intelligence/law enforcement dichotomy[214] that underlay what the government sought to obtain in FISA was of long standing. FISA merely continued that government-originated dichotomy. Nor was this dichotomy especially problematic. It had not generally been difficult to identify which surveillances were "intelligence" surveillances and which were "law enforcement" surveillances in previous years for a variety of historical and institutional reasons. This, of course, did not mean that information that was evidence of crimes that was obtained could not be used or that information which was both intelligence information and evidence of crimes could not be sought. There remained a discernible

[213] *See, e.g.*, *S. 1448, the Intelligence to Prevent Terrorism Act of 2001 and Legislative Proposals in the Wake of the September 11, 2001 Attacks*, *supra* note 64, at 29, 32–33, 36–37.

[214] The Review Court cites the government for referring to "the false dichotomy between foreign intelligence information that is evidence of foreign intelligence crimes and that which is not." *In re Sealed Case*, 310 F.3d at 725. Nothing I say here is intended to disagree with the government's characterization. FISA did not distinguish between foreign intelligence information that was evidence of foreign intelligence crimes and foreign intelligence information that was not evidence of crimes. That false dichotomy was invented by OIPR, not by FISA or *Truong*. What FISA and *Truong* distinguished between was surveillances for the purpose of law enforcement and surveillances for the purpose of obtaining foreign intelligence.

difference between a surveillance undertaken specifically to enforce the criminal law and a surveillance undertaken to obtain intelligence information that might sometimes lead to criminal prosecutions.

Moreover, nothing in FISA required "the wall" that subsequently was erected first by OIPR and later the FISC minimization procedures. Indeed, to the extent "the wall" frustrated both intelligence activities and the use of evidence in criminal prosecutions of information acquired in foreign intelligence surveillances, "the wall" was contrary to the language in FISA intended to assure the ability to use such information in criminal cases. In other words, the problems that motivated the post-9/11 FISA amendments were not properly caused by FISA or its primary purpose requirement. Even in the absence of those amendments and even if the Review Court had correctly recognized that FISA contained a "primary purpose" requirement, that court still should have and would have overturned the FISC minimization procedures as unauthorized by FISA.

Nonetheless, as interpreted here, the original FISA did limit the purpose of a FISA surveillance. Even if that limitation normally should not cause problems either for intelligence agencies or law enforcement, because as properly construed the limitation placed little constraint on consultation and coordination and no limitation on use in criminal trials of the information obtained, the limitation clearly did cause problems because it was misconstrued. Clarification of the original intent would have been one response, but amendment to eliminate or lessen that limitation was another possible response—and it was the response taken. The immediate aftermath of 9/11, however, was not the best situation in which to consider calmly either the necessity or all the ramifications of a change to the purpose requirement. Accordingly, the temporary amendment of "the purpose" requirement into "a significant purpose" requirement was a measured response. Unfortunately, there does not appear to have been any serious consideration given to the issue before the provision was made permanent in 2005.

What are the implications of such a change? It is clear that FISA now constitutes a system by which the government can intentionally subject a person to the most wide-ranging and intrusive searches to obtain evidence of criminal behavior for the purposes of using it in a criminal prosecution, absent the traditional safeguards associated with searches for evidence of crimes. The question is whether the safeguards that do exist in FISA are sufficient in terms of both the Fourth Amendment and good public policy. In an area of national security, determinations agreed to by both political branches, in an apparent attempt to balance the needs of national security with individual liberties, are unlikely to be overturned by courts on the basis of the Fourth Amendment. That is, one should not place much hope in the courts second-guessing political determinations in this area. Rather, for better or for worse, the appropriate safeguards will have to be determined in the political arena.

Whether FISA as amended is the most appropriate balance between the interests of national security and individual liberties is beyond the

scope of this Article. It has been the subject of a number of articles[215] and undoubtedly will be the subject of more, especially if FISA is further amended to address the NSA surveillances and to update the definition of "electronic surveillance" in FISA.[216] What I hope this Article may contribute to that consideration is a recognition that the primary purpose requirement was incorporated into the original FISA, and that requirement did not, properly construed, and as it was in fact construed for the first fifteen years, create any meaningful obstacle to either intelligence or law enforcement activities against clandestine intelligence activities or international terrorism. At the same time, the primary purpose requirement was not incorporated as an intentional safeguard against using FISA for law enforcement purposes, but as an assumed requirement for a surveillance not authorized by a traditional warrant based upon probable cause that a crime was being, or had been, committed. That assumption was based, not without substantial foundation, on case law that seemed to distinguish between searches for law enforcement purposes that would require traditional warrants and searches for intelligence purposes that could be authorized on a non-traditional warrant basis, if not on Presidential authorization alone.

In the current environment, it may be that an explicit provision authorizing electronic surveillance that is not intended to be primarily for intelligence purposes, but instead is intended to be used equally for law enforcement as well as intelligence purposes, as now contained in FISA, is appropriate. However, this Article has hopefully demonstrated that elimination of a "primary purpose" requirement is not necessary to facilitate coordination and cooperation between law enforcement and intelligence agencies. If the elimination of the "primary purpose" requirement is to be justified, if must be on a different basis.

[215] *See supra* note 16.

[216] It is amazing that FISA has worked as well as it has without significant amendment of this definition since 1978, when there were neither cell phones nor the Internet.