

What NSA Is Doing . . . and Why It's Illegal

by JOHN CARY SIMS*

Introduction

On December 16, 2005, *The New York Times* disclosed the existence of a secret electronic surveillance program being carried out by the National Security Agency (NSA) that involves warrantless interception of the contents of international communications engaged in by “United States persons” – citizens of the United States and aliens admitted for permanent residence.¹ Although details of exactly what NSA is doing have not been officially disclosed, the President, the Attorney General, and the former director of NSA (who has now become the Director of the Central Intelligence Agency) have all acknowledged that a new “Terrorist Surveillance Program” that goes beyond the boundaries previously respected was initiated in October 2001.² Even without the factual predicates that would make debate

* Professor of Law, University of the Pacific, McGeorge School of Law; Co-Editor-in-Chief, *Journal of National Security Law & Policy*. This article is based upon a presentation made at the Hastings College of the Law on March 29, 2006. I am grateful for the research assistance provided by Joshua D. Moore (Pacific McGeorge Class of 2007).

1. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1. This article will not analyze another NSA program that has been more recently described, which consists of the analysis of large quantities of information about domestic telephone calls, but without acquisition by the government of the contents of the calls. See Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls; 3 Telecoms Help Government Collect Billions of Domestic Records*, USA TODAY, May 11, 2006, at 1A. Such data-mining raises interesting and important issues, but they are distinct for the most part from those addressed here. See Letter from William E. Moschella, Assistant Attorney General, U.S. Department of Justice, to F. James Sensenbrenner, Jr., Chairman, Committee on the Judiciary, U.S. House of Representatives, *Responses to Questions from Chairman Sensenbrenner*, March 24, 2006, at 37 [hereinafter DOJ Responses to House Judiciary Committee] (“the Terrorist Surveillance Program is *not* a ‘data-mining’ program”) (emphasis in original), available at <http://www.fas.org/irp/agency/doj/fisa/doj032406.pdf>.

2. See, e.g., DOJ Responses to House Judiciary Committee, *supra* note 1, *Responses to Questions from Chairman Sensenbrenner*, at 25 (“The Program was first authorized and implemented in October 2001.”). The Justice Department has indicated that it is not aware of any prior occasion, since the passage of the Foreign Intelligence Surveillance Act in 1978, in which authorization was given for “electronic surveillance” as defined in the

about the legality of the program a more illuminating and satisfying endeavor, there have been numerous efforts to describe and analyze the once-secret surveillance efforts and assess their legality.³ This article will provide a more detailed description than has previously been available of exactly what it is that NSA is doing. Once the nature of the program is more clearly understood, the conclusion that it violates the law as it stands is unavoidable.⁴

I. Title III, *Keith*, and FISA

The Fourth Amendment to the United States Constitution states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.⁵

Act without obtaining a warrant. *Id.*, *Responses to Joint Questions from House Judiciary Minority Members*, at 11.

3. For example, the Department of Justice has prepared and widely disseminated a 42-page memorandum supporting the program. U.S. DEPARTMENT OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT, Jan. 19, 2006, available at <http://www.fas.org/irp/nsa/doj011906.pdf>. The view that the program is plainly illegal was presented in an answering letter signed by over a dozen distinguished law professors and former government officials. Letter to Bill Frist, Majority Leader, U.S. Senate, et al., from Curtis A. Bradley, Richard and Marcy Horvitz Professor of Law, Duke University, et al., Feb. 2, 2006, available at http://www.law.duke.edu/publiclaw/pdf/second_letter.pdf.

4. The Senate Judiciary Committee has held a number of hearings to explore the program, and one possible legislative response under consideration would be to amend the Foreign Intelligence Surveillance Act to permit court approval of surveillance programs designed to accomplish the purposes identified by the Bush administration as justifying the ongoing program, with the requirement that the ongoing program then be promptly submitted for review. See S. 2453, 109th Cong., 2d Sess. (2006) (sponsored by Sen. Specter, Chair of the Senate Judiciary Committee); Walter Pincus, *Specter Offers Compromise on NSA Surveillance*, WASH. POST, June 9, 2006, at A4 (describing a revised proposal introduced by Senator Specter at a meeting of the Senate Judiciary Committee); Editorial, *NSA Train Wreck; An Effort To Get NSA Surveillance Under Control Is Morphing into a License To Spy*, WASH. POST, June 12, 2006, at A20 (“In an effort to win votes, Mr. Specter has turned [S. 2453] from a flawed accountability measure into one that rewrites the rules of domestic surveillance and gives the administration an all but blank check to spy.”).

5. U.S. CONST. amend. IV.

The Supreme Court has recognized that electronic eavesdropping, even in the absence of physical intrusion, may constitute a search within the meaning of the Fourth Amendment.⁶ In recognition of the threat to privacy interests posed by electronic surveillance, Congress in 1968 enacted Title III of the Omnibus Crime Control and Safe Streets Act.⁷ Title III established detailed requirements for the issuance of federal and state warrants authorizing electronic intercepts, and the statute also created an elaborate system for keeping records of and making reports about electronic surveillance.⁸ In national security matters such as those involved in the fight against terrorism, the federal government may at any time avail itself of the Title III process to obtain warrants based on a showing of probable cause that serious crimes have been committed or are about to be committed.⁹ However, the Executive rejects such close judicial supervision of national security interceptions, based on the contention that such limitations on the President in the intelligence field are inconsistent with his responsibilities for national defense and foreign relations. The present controversy is only the latest chapter in a long-running effort by Presidents to undertake electronic surveillance for national security purposes without the necessity to obtain Title III warrants, and indeed to resist the application of any warrant requirement in a number of situations.

An occasion to explore the applicability of the Title III restrictions on electronic surveillance to national security matters was presented to the Supreme Court in *United States v. United States District Court*,¹⁰ often referred to as the “Keith” case because then District Judge Damon J. Keith¹¹ became the subject of an application for a writ of mandamus filed by the government to challenge the district court’s order requiring disclosure of certain electronic surveillance information. The court of appeals upheld the district court’s ruling. The case involved national security, since one

6. *Katz v. United States*, 389 U.S. 347 (1967).

7. 82 Stat. 213 (1968), *codified at* 18 U.S.C.A. §§ 2510-2520 (2000 & Supp. 2006).

8. Annual reports are prepared by the Administrative Office of the United States Courts for transmittal to Congress. 18 U.S.C. § 2519(3) (2000). The most recent report indicates that in 2005, a total of 1,773 intercept orders were approved, of which 625 were issued by federal courts. ADMINISTRATIVE OFFICE OF THE U.S. COURTS, 2005 WIRETAP REPORT 5 (2005), *available at* <http://www.uscourts.gov/wiretap05/contents.html>.

9. 18 U.S.C. § 2518(3) (2000).

10. 407 U.S. 297 (1972).

11. Judge Keith was later appointed to the United States Court of Appeals for the Sixth Circuit, where he now is a senior judge.

defendant was accused of bombing an office of the Central Intelligence Agency in Ann Arbor, Michigan,¹² but the perceived threat did not arise from the activities of foreign powers. The Attorney General described the warrantless surveillance as designed “to protect the nation from attempts of *domestic organizations* to attack and subvert the existing structure of Government.”¹³ The government took the position that it was unnecessary to obtain Title III warrants in such domestic security cases, but the Supreme Court rejected its arguments and affirmed the judgment of the court of appeals.

The *Keith* decision is highly relevant to the analysis of the current surveillance program, but it also left a number of important questions unanswered. The government relied heavily on the language then contained in Title III that stated that the statute should not “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.”¹⁴ Although the government argued that this language excepted all national security wiretaps from Title III, the Supreme Court concluded to the contrary that “Congress simply left presidential powers where it found them.”¹⁵ The Court recognized that national security concerns raised by the government were serious,¹⁶ and that domestic security surveillance “may involve different policy and practical considerations from ‘ordinary crime,’”¹⁷ but the Court ultimately concluded that advance approval of electronic surveillance by a neutral and detached judicial officer is required in domestic security matters.¹⁸ Even so, the Court made it clear that its holding applied only to domestic security matters, not those involving foreign intelligence:

12. *Keith*, 407 U.S. at 299, 308.

13. *Id.* at 309 (emphasis supplied by the Supreme Court in quoting the affidavit of the Attorney General).

14. *Id.* at 302, quoting 18 U.S.C. § 2511(3). This language was later repealed. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 201(c), 92 Stat. 1783, 1797.

15. *Id.* at 303.

16. *Id.* at 311.

17. *Id.* at 322.

18. *Id.* at 317 (“unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech”).

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.¹⁹

While disclaiming any intent to guide congressional action, the Supreme Court then proceeded in *Keith* to suggest a possible way of reconciling a warrant requirement with the practicalities of the intelligence field. The Court observed that standards for the issuance of a warrant “may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.” This might lead Congress to conclude that new warrant requirements should be crafted that would be “more appropriate to domestic security cases,” that authorization could be given by “any member of a specially designated court,” and that the time and reporting requirements of Title III could be relaxed.²⁰ This stunningly prescient (or persuasive) formulation by the Supreme Court provides the backbone of the legislative compromise over *foreign* intelligence surveillance that became the Foreign Intelligence Surveillance Act of 1978 (FISA).²¹ Even though the rough blueprint drawn up the Supreme Court in *Keith* closely resembles the system created by Congress in FISA, Congress has never seen the need to override the holding of *Keith* as to domestic security cases, which remain subject to the restrictions of Title III.

Between the Supreme Court’s decision in *Keith* and the enactment of FISA in 1978, Congress devoted substantial attention to infringements of civil liberties by agencies of the United States, particularly the Central Intelligence Agency, the Federal Bureau of Investigation, and NSA. The Watergate hearings, as well as the investigations of the Church Committee and the Pike Committee, exposed numerous abuses of power. Most significantly for present purposes, the revelations covered the use of break-ins and electronic surveillance against United States citizens based on their exercise of First Amendment rights. The exposure of NSA “watch lists” targeting antiwar protestors bolstered efforts to make national security surveillance subject to statutory standards. Development of a statutory system was also stimulated by the constitutional ambiguity generated by *Keith*. Supporters of reform hoped, and generally

19. *Id.* at 321-22.

20. *Id.* at 323.

21. Pub. L. No. 95-511, 92 Stat. 1783, *codified at* 50 U.S.C.A. §§1801-1811 (2003 & Supp. 2005).

predicted, that when the Supreme Court was presented with a case involving warrantless electronic surveillance in a foreign intelligence matter it would conclude that it would not be consistent with the Fourth Amendment for the Executive to be permitted to conduct even national security “searches” without judicial supervision. The Executive, on the other hand, took heart from *Keith*’s explicit announcement that the holding did not apply to foreign security cases, and the suggestion that warrants might not be needed in cases involving foreign powers.²² At the same time, *Keith*’s recital of the threat to personal liberties posed by allowing surveillance to be put in place on the basis of “unreviewed executive discretion”²³ seemed to be as applicable to foreign intelligence wiretaps as to those directed at domestic security threats.

Extensive congressional deliberation, in the shadow of the risks that each side saw in the potential for an ultimate Supreme Court decision to go against it on the central question left open in *Keith*, led to FISA. This is not the occasion to thoroughly canvass the statute, but the basic approach taken in foreign intelligence cases was that suggested by the Court in *Keith* as a possible solution to the problem of domestic security wiretaps. Warrants would be required, but they would not be Title III warrants based on probable cause that a crime had been committed or was imminent. Rather, warrants would be justified upon a showing that there was probable cause to believe that the target is a foreign power or the agent of a foreign power.²⁴ This is uniformly agreed to be a standard that is easier to meet than the Title III standard.

Applications for FISA warrants go to the Foreign Intelligence Surveillance Court (FISC), a special court created by the statute, made up of eleven Article III district court judges who are designated by the Chief Justice of the United States to carry out the additional duties of judges of the FISC.²⁵ An application for a FISA warrant is considered

22. *Keith*, 407 U.S. at 322 & n.20.

23. *Id.* at 317.

24. 50 U.S.C.A. § 1805 (2003 & Supp. 2005). The definition of “foreign power” includes “a group engaged in international terrorism or activities in preparation therefor.” *Id.* at § 1801(a)(4). Eventually it was recognized that electronic surveillance might also be appropriate if directed at an international terrorist who is not affiliated with a foreign power. This problem was addressed, despite the grammatical awkwardness, by *defining* such a lone wolf to be an “agent of a foreign power.” *Id.* at § 1801(b)(1)(C).

25. *Id.* at § 1803(a). Prior to passage of the USA PATRIOT Act in 2001, the FISC had seven judges. The statute also provides for a court of review, made up of three Article III judges designated by the Chief Justice. *Id.* at § 1803(b).

by a single judge, with a rotation set up to assure that a judge is always available in or near Washington, D.C. to consider an application that requires immediate attention.²⁶ The statute requires that annual reports be sent to the Administrative Office of the United States Courts, although the information provided is much less detailed than in the reports required by Title III.²⁷

II. How NSA Operates

Those who go to the movies or read spy novels are frequently exposed to the hypothesis that the National Security Agency listens in on all private electronic communications at will, whether they are conducted by telephone, fax, or e-mail. A near-omniscience is attributed to the organization, except for communications that are kept out of the air altogether, such as by being delivered in personal conversation, by hand, or through the mails. One focus of concern, especially in Europe, has been the system code-named "Echelon," which was described in a report to the European Parliament as being "designed to indiscriminately intercept the non-military communications of governments, private organizations, and businesses on behalf of the United States and its primary partners in the decades-old UKUSA signals intelligence alliance – Britain, Australia, Canada, and New Zealand. Items of intelligence value are selected by computer identification of keywords provided by the UKUSA nations."²⁸

26. At least three of the judges reside within twenty miles of the District of Columbia. *Id.* at § 1803(a).

27. The most recent report indicates that during 2005 a total of 2,074 applications were made to the FISC for warrants to conduct electronic surveillance, make physical searches, or both. Two applications were withdrawn before they were ruled on; 2,072 applications were granted, with 61 of those having been the subject of substantive modifications by the court; no application was denied in whole or part. Letter to J. Dennis Hastert, Speaker, U.S. House of Representatives, from William E. Moschella, Assistant Attorney General, U.S. Department of Justice, April 28, 2006, *available at* <http://www.fas.org/irp/agency/doj/fisa/2005rept.html>.

28. Jeffrey Richelson, *Desperately Seeking Signals; The National Security Agency's Echelon Program*, BULL. ATOMIC SCI., March/April 2000 (Vol. 56, No. 02), at 47. Richelson persuasively demonstrates that "Echelon" is only one aspect of the NSA's interception of communications, and that the innovation it represents is the large-scale computerized exchange among the cooperating nations of raw intercepts, as opposed to finished reports. His short article also provides an excellent overview of the activities of NSA. Although the agency was once so obscure that it was appropriate to joke that its initials were an acronym for "No Such Agency," there is now a substantial body of published work about it. *See, e.g.*, JAMES BAMFORD, BODY OF SECRETS: ANATOMY OF THE ULTRA-SECRET NATIONAL SECURITY AGENCY (Anchor 2002); JAMES BAMFORD, THE PUZZLE PALACE: A REPORT ON AMERICA'S MOST SECRET AGENCY (1982);

Even given NSA's immense human and computer resources, interception and analysis of all electronic communications is not possible.²⁹ A first obstacle is the immense volume of electronic communication, including telephones (landlines and cellular), e-mails, and other forms. General Michael V. Hayden, who directed NSA for six years before becoming Principal Deputy Director of National Intelligence, and more recently Director of the CIA, has testified that the "explosion in telecommunications" has brought about a situation in which the percentage of signals collected by NSA, relative to the overall volume of signals, has "never been smaller."³⁰ A second significant practical difficulty is that many communications, and certainly a significant percentage of those of primary interest to the U.S. intelligence community, are not in English, and few competent linguists may be available to work in the critical languages.³¹ Third, the communications may be encrypted or encoded; this is certainly not a new problem, but one that is exacerbated by the ready

PATRICK RADDEN KEEFE, CHATTER: DISPATCHES FROM THE SECRET WORLD OF GLOBAL EAVESDROPPING (2005); Lawrence D. Sloan, *ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 DUKE L.J. 1467 (2001).

29. This discussion addresses only technical feasibility. There also are legal limits, which will be discussed below.

30. *The National Security Agency: Hearing Before the House Permanent Select Committee on Intelligence*, April 12, 2000 (Lexis, News Library) [hereinafter *Hayden 2000 House Testimony*] (testimony of Gen. Hayden); see also *id.* ("Our ability to collect may have increased, but it has increased at a pace far slower and smaller than the explosion of the 1s and 0s that are out there."); JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION 48 (2006) ("Today, industry experts estimate that approximately 9 trillion e-mails are sent in the United States each year. Americans make nearly a billion cell phone calls and well over a billion landline calls each day."); Richelson, *supra* note 28 ("The UKUSA SIGINT agencies certainly do not intercept every signal that passes through the airwaves."). SIGINT is "signals intelligence," a term that was defined by General Hayden in his prepared remarks for the House Intelligence Committee hearings on April 12, 2000: "Signals intelligence is comprised of communications intelligence and electronics intelligence. Communications intelligence consists of foreign communications passed by radio, wire, or other electromagnetic means and electronics intelligence consists of foreign electromagnetic radiations such as emissions from a radar system." Michael V. Hayden, *Statement for the Record*, Hearing Before the House Permanent Select Committee on Intelligence, April 12, 2000, at 6 n.4, available at http://www.fas.org/irp/congress/2000_hr/hayden.html.

31. See James Bamford, *The Agency That Could Be Big Brother*, N.Y. Times, Dec. 25, 2005, § 4 (Week in Review), at 1:

During the cold war, the agency could depend on a constant flow of American-born Russian linguists from the many universities around the country with Soviet studies programs. Now the government is forced to search ethnic communities to find people who can speak Dari, Urdu or Lingala – and also pass a security clearance that frowns on people with relatives in their, or their parents', former countries.

availability of encryption software to private individuals.³² Another difficulty is the “significant limit imposed on the ability to monitor voice communications” because of the ineffectiveness of computerized systems for spotting words in aural communications.³³ General Hayden has noted that this problem may not be as urgent as it once was, since “E-mail is a bit going back to the future, looking a lot more like telex, which is the roots of our organization, reading the printed word, rather than the recent past of our organization, which is dealing with the spoken word.”³⁴ A fifth concern is that some signals may also be difficult for NSA to acquire, or perhaps unavailable altogether, because they are transmitted through fiber-optic cables rather than being sent through the air by microwave or satellite.³⁵

Despite all the difficulties faced by NSA, it remains true that “NSA and its allies clearly do intercept an enormous volume of data.”³⁶ In testimony before the House Permanent Select Committee on Intelligence in 2000, General Hayden addressed concerns raised by the American Civil Liberties Union that NSA’s capabilities could be used against Americans. His statement emphasized that there are “absolutely clear rules” prohibiting such practices, but went on to make a point that is highly pertinent in analyzing the agency’s

32. The availability of more powerful personal computers and the development of public key cryptography made it practicable for private parties to use effective encryption at low cost. *See, e.g.,* Seymour M. Hersh, *The Intelligence Gap: How the Digital Age Left Our Spies Out in the Cold*, *NEW YORKER*, Dec. 6, 1999, at 58 (reporting that “the agency’s long fight against encryption delayed its widespread use by many years” but that “encryption could not be stopped”).

33. Richelson, *supra* note 28 (“In 1993, former NSA director Bobby Inman admitted that ‘I have wasted more U.S. taxpayer dollars trying to do that [word spotting in speech] than anything else in my intelligence career.’”). Whatever limitations exist on the effectiveness of voice transcription systems would not prevent NSA from acquiring and recording a given telephone conversation, but the incentive to engage in any given surveillance program is substantially reduced if it requires a large investment of resources (such as the use of a linguist) to convert the content of the call into usable form. Richelson notes that even in the absence of effective word spotting by computers, “the phones of the parties involved in a call can be automatically identified and voiceprints can be used to identify who is speaking.” *Id.* Even if one assumes that Inman’s 1993 statement was accurate, it remains possible that a breakthrough has been achieved since that time. *See* BAMFORD, *BODY OF SECRETS*, *supra* note 28, at 556 (“A recent breakthrough was made by biomedical engineers at the University of Southern California, who claim to have created the first machine system that can recognize spoken words better than humans can.”).

34. *Hayden 2000 House Testimony*, *supra* note 30.

35. Richelson, *supra* note 28.

36. *Id.*

technological limitations as well as the legal constraints under which it operates. He stated:

There is a powerful element of truth in the ACLU text, okay. And that talks about opportunity or capability. For us to do our mission in today's telecommunications world requires a substantial amount of capability, okay. It's theoretically possible for us to use that capability – technologically possible to use that capability in ways that are prohibited. Of course I have to answer yes.³⁷

All informed observers agree that the ability of NSA to intercept electronic communications is very large, even if it is not effectively unlimited, as is sometimes alleged. Thus, in exploring the legal issues raised by the recent NSA electronic surveillance program, it is prudent to assume that almost any electronic communication that is sent through the air can be acquired by NSA if it is deemed to be worth the effort.³⁸

That brings us to the aspect of its operations that NSA guards most closely. Since it has the technical capacity to intercept a large percentage of the electronic communications that flood the modern world,³⁹ but it cannot with the available personnel and other resources intercept and analyze all of them, it must set priorities. Day in and

37. *Hayden 2000 House Testimony*, *supra* note 30.

38. NSA's access to communications transmitted on fiber-optic cables remains unknown, but it has recently been alleged that it taps into the cables "by using specially designed submarines, such as the USS *Jimmy Carter*, to attach a complex 'bug' to the cable itself." James Bamford, *Big Brother Is Listening*, ATLANTIC MONTHLY, April 2006, at 65, 68; see KEEFE, *supra* note 28, at 73-75. It has also been alleged that NSA has been granted direct access to the networks of telecommunications carriers, making it unnecessary to seek to obtain signals from fiber-optic cables. See, e.g., *id.* at 68 (stating that fiber-optic cables entering the United States from Europe and Asia are tapped at the landing stations where they come ashore); Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove*, *Officials Report*, N.Y. TIMES, December 24, 2005, at A1 (reporting that NSA "has gained the cooperation of American telecommunications companies to obtain backdoor access to streams of domestic and international communications" and that the agency has "in the last few years been quietly encouraging the telecommunications industry to increase the amount of international traffic that is routed through American-based switches"). Communications sent by fiber-optic cables would also be vulnerable to interception if sent through the air at any point in their path from sender to recipient.

39. The degree of success that NSA achieves in its efforts to keep up with the ever-growing flood of electronic communications is disputed. Compare note 30 *supra* and accompanying text and Hersh, *supra* note 32, with Bamford, *supra* note 38, at 70 (stating that NSA personnel "are close to achieving" their "ultimate goal of intercepting and reviewing every syllable and murmur zapping into, out of, or through the United States").

day out, NSA must make decisions about what communications it will intercept, which ones it will store for future reference, which ones it will subject to preliminary screening by computers, which ones will be routed for inspection by a human analyst, and ultimately which ones will be given a full analysis that will be transmitted to its “customers” in the intelligence community, including the President. As General Hayden has stated, “there is a great demand that we focus what it is that we can work against on the highest-priority legitimate foreign intelligence targets we have.”⁴⁰ Plainly, the effectiveness of NSA’s efforts could be greatly diminished if it were known what channels of communications it is intercepting, or which ones it places special emphasis on, or for that matter which ones it has decided are not worth the effort to intercept and analyze. Those who wished to avoid detection would choose modes or channels of communication that are not monitored, or that receive low emphasis from NSA. On the other hand, one hostile to the United States who knows that a given channel is being closely monitored may deliberately transmit false information or otherwise act to manipulate U.S. responses.⁴¹

The setting and implementation of priorities is at the very heart of what NSA does. It can focus on particular modes or channels of communication, particular locations, particular phone numbers or e-mail addresses, characteristics of the communication (e.g. length, language, use of encryption), and content, such as particular names, words, phone numbers, or combinations of these.⁴² No doubt

40. *Hayden 2000 House Testimony*, *supra* note 30.

41. There is no limit to the permutations that are possible. James Bamford had reported that (at least as of the time he collected information for his most recent book) “NSA regularly listens to unencrypted calls from suspected terrorist Osama bin Laden, in hiding in Afghanistan,” that bin Laden “is aware that the United States can eavesdrop on his international communications, but he does not seem to care,” and that NSA analysts “play audiotapes of Bin Laden talking to his mother” in order to impress visitors. BAMFORD, *BODY OF SECRETS*, *supra* note 28, at 410. In the Afterword to the paperback edition of the book, Bamford states that bin Laden changed tactics in 1998 after “an American missile attack on his compound in Afghanistan made him think twice about using satellite communications.” *Id.* at 614. He alleges that since that time bin Laden has communicated through messengers who make calls for him, and that even so NSA intercepted a call in early September 2001 from a bin Laden associate to bin Laden’s wife, urging her to return to Afghanistan from Syria. *Id.* at 616-17. Bamford indicates that the call “was filed away” without its significance being recognized. *Id.* at 617.

42. Jeffrey Richelson reports that, at least in the context of the discussion of the “Echelon” program, screening of content is accomplished through the use of “dictionaries” of keywords. Richelson, *supra* note 28. A simple version of keyword screening would be compilation of a “watch list” like those used by NSA in the programs investigated by the Church Committee, in which communications by, to, or about certain individuals were targeted. James Bamford contends that a computer, codenamed

communications between Russia and the Russian embassy in Washington have long been the target of intense focus by NSA. Thus, an effort might well be made to acquire and store every possible communication, even those that are encrypted at a high level. After 9/11, there can be no doubt about the fact that communications between the United States and such nations as Afghanistan, Iraq, Iran, Pakistan, and Saudi Arabia have been very high on NSA's list of priorities. It may well be that all accessible international phone calls and e-mails are screened to some extent, but it would seem plausible that calls between England and France would receive less emphasis than those between Afghanistan and Europe, or calls within the Middle East. NSA no doubt can acquire radio communications by taxicabs around the world, but whether it wants to do so absent a specific reason is another matter. NSA has an enormous appetite for electronic transmissions, but it still must make choices rather than ordering everything on the menu. Although the transcription of this testimony by General Hayden is a bit garbled, he captures the essence of the difficult task that NSA is attempting to carry out as it processes the messages that it has intercepted:

We collect far more information than we process, analyze far more – process more than we analyze and report less than we – *it's a funnel, and it narrows*. And [an intercept] may never come to our attention, and be shunted off and destroyed in that sense, without the intervention of any of our operators.⁴³

An additional window into NSA's processing of the flood of signals it intercepts was provided by an incident that began on

Dictionary, searches for "keywords, names, phrases, telephone and fax numbers." BAMFORD, BODY OF SECRETS, *supra* note 28, at 409. The basics of the screening process can easily be imagined by one familiar with the Lexis and Westlaw legal research systems, or even with the broad searching possible through Google.

43. *Hayden 2000 House Testimony*, *supra* note 30 (emphasis added). General Hayden was responding to a question about what would happen to an intercept containing "inadvertent information on an American," but his description of how intercepts are processed appears to be generally applicable. One of General Hayden's predecessors as director of NSA described a collection system that generated a million inputs per hour, with the following results: "filters throw away all but 6,500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report is produced." Sloan, *supra* note 28, at 1480 (quoting a 1992 speech by Vice Admiral William Studeman).

January 24, 2000, when NSA's computer system crashed.⁴⁴ General Hayden described the problem and NSA's recovery from it in his congressional testimony:

[I]t's been in the press, about the outage at NSA in late January. You know, a serious matter in which we have already stated publicly for three and a half days we could not process information.

But I've also stated publicly the collection systems continued, and that we had the ability to store that which we collected over this three and a half day period. And that when we then were able to go back and process the information when that capability came back, it took eight to 12 hours to process and analyze the information that we had collected and life got closely – in a close sense, back to normal.⁴⁵

NSA's mission, activities, resources, and culture are central elements in the current controversy over warrantless surveillance of the international electronic communications of United States persons who are within the United States. The capacity of the agency to intercept such communications is very broad, but the flow of data is also enormous because of recent advances in communications. The key to success is for NSA to tailor its targeting priorities to the needs of the intelligence community, while keeping those priorities secret from the targets and dealing with any technical problems that might impair access to the desired signals. Patrick Radden Keefe has aptly described "the intelligence cycle" that governs the work of NSA and other agencies:

The cycle starts with planning and target selection, which then leads naturally to collection of raw intelligence. Next, the collected intelligence goes through processing, then analysis and production of finished intelligence

44. See BAMFORD, *BODY OF SECRETS*, *supra* note 28, at 451-54.

45. *Hayden 2000 House Testimony*, *supra* note 30; see KEEFE, *supra* note 28, at 109-10; BAMFORD, *BODY OF SECRETS*, *supra* note 28, at 454 (reporting that, during the outage, much of the intercept traffic that would have normally gone to NSA was directed instead to the agency's British counterpart, GCHQ).

reports, and ultimately distribution to interested parties, before starting back at the planning stage again.⁴⁶

While Keefe is describing the process in terms applicable to any intelligence agency, it accurately describes what NSA does in intercepting communications and then processing and analyzing them in order to produce finished reports for distribution. The one additional aspect of NSA's work that needs to be described in order to permit an appropriate analysis of the warrantless surveillance program is the legal framework within which NSA operates.

III. How Did NSA Handle Information About U.S. Persons Before the New Warrantless Surveillance Program Was Put in Place?

The central component of the intricate system created by FISA to regulate electronic surveillance is the concept of "agent of a foreign power." The FISC judge to whom an application is made cannot issue a FISA warrant unless, in addition to finding that all the other requirements of the statute have been complied with, the judge finds that

on the basis of the facts submitted by the applicant there is probable cause to believe that –

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power⁴⁷

46. KEEFE, *supra* note 28, at 109-10.

47. 50 U.S.C.A. § 1805(a)(3) (2003 & Supp. 2005). There are many details in FISA that do not call for discussion here. However, it is worth noting that the Attorney General may authorize certain electronic surveillance without the need to seek a FISA warrant, primarily when the target is an embassy or similar facility of a foreign nation. *Id.* at § 1802. In addition, the language of section 1805(a)(3)(A) quoted in the text omits an important proviso designed to guard against abuses of the sort that NSA had committed in the past: "Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States."

Much turns, then, on the statutory definition of “an agent of a foreign power,” since no individual may be subjected to electronic surveillance that requires a FISA warrant unless there is probable cause to believe that the person is such an agent. The statutory definition is itself complex, but for present purposes it is only necessary to explore when a United States person is considered an agent of a foreign power.⁴⁸ An individual is a “United States person” if a citizen or an alien lawfully admitted for permanent residence.⁴⁹ A United States person is an agent of a foreign power if he or she “knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States,”⁵⁰ or if he or she “knowingly” engages in similar activities that are obviously inimical to the interests of the United States.⁵¹ For purposes of our discussion here, let us assume that the potential subject of electronic surveillance is a United States person who could potentially fall within the quoted portion of the definition.

Before we plunge more deeply into how the warrantless electronic surveillance program should be analyzed as applied to the United States person described above, it will be useful to identify a number of situations that plainly do not fall within the scope of the program as it has been described to the public. For purposes of this discussion, let us assume that the communications in question take place “under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law

48. The standard for so labeling those who are not United States persons is more expansive. *Id.* at § 1801(b)(1). Any person, whether or not a United States person, is an agent of a foreign power if he or she meets the narrower definition applicable to United States persons. *See id.* at § 1801(b)(2).

49. *Id.* at § 1801(i). The definition also describes when an unincorporated association or a corporation is a United States person.

50. *Id.* at § 1801(b)(2)(A).

51. *Id.* at § 1801(b)(2)(B)–(E). These additional categories of agents of foreign powers include those who knowingly engage in certain clandestine intelligence activities at the direction of and on behalf of a foreign power; knowingly engage in sabotage or international terrorism or preparation therefore; knowingly use a false identity on behalf of a foreign power; or knowingly aid or abet, or conspire to engage in, the activities described in the first three parts of the definition. General Hayden succinctly summarized the complex statutory definition: “a judge may determine a U.S. person to be an agent of a foreign power only if there is information to support a finding that the individual is a spy, terrorist, saboteur, or someone who aids or abets them.” Hayden, *Statement for the Record*, *supra* note 30, at 3.

enforcement purposes.”⁵² This discussion will be limited to situations that *do not* fall within *any* of the following categories:

- A Title III warrant has been issued.⁵³
- A FISA warrant has been issued.⁵⁴
- The United States person in question is outside the United States.⁵⁵
- The government does not intend to intercept the contents of the communication.⁵⁶
- The interception occurs within the United States.⁵⁷

52. 50 U.S.C.A. § 1801(f)(1), (3)–(4). This is certainly an appropriate assumption for telephone calls, faxes, and e-mails.

53. The essence of the FISA legislative compromise was to give the government a way to obtain a warrant for electronic surveillance that did not require meeting the probable cause standard applied in ordinary criminal cases. Therefore, in the hypothetical situation described in the text the government would not choose to take upon itself the higher burden of seeking a Title III warrant.

54. The current controversy has arisen precisely because the government has chosen not to seek FISA warrants. If FISA warrants were sought, some might be denied. Most, but not all, applications for FISA warrants have been granted.

55. United States persons who are outside the United States were explicitly excluded from the reach of FISA. *See, e.g.*, 50 U.S.C.A. § 1801(f)(1) (defining “electronic surveillance” as the acquisition of the contents of certain communications to or from “a particular, known United States person who is in the United States”). At the time FISA was adopted, a number of those involved in the deliberations stated that additional legislation would be crafted to deal specifically with United States persons outside the United States, *see, e.g., Foreign Intelligence Surveillance Act of 1978: Hearings Before the Subcommittee on Intelligence and the Rights of Americans of the S. Comm. on Intelligence*, 95th Cong. 39 (statement of Attorney General Griffin Bell) (“The next item of priority is electronic surveillance of Americans overseas. We’ve agreed to do that next.”), but no such legislation has ever been adopted. Executive Order 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), requires approval from the Attorney General before NSA interception can be targeted against United States persons outside the United States. *Id.* at § 2.5.

56. The statutory definition of “electronic surveillance” includes only the acquisition “of the contents” of a wire or radio communication. 50 U.S.C.A. § 1801(f)(1)–(3).

57. Acquisition of wire communications to or from a person in the United States, when the interception occurs in the United States, is included in the definition of “electronic surveillance,” and thus requires a warrant, unless a party to the communication has given consent. There is a narrow exception applicable to communications of computer trespassers. *Id.* at § 1801(f)(2), referring to 18 U.S.C. § 2511(2)(i) (2000 & Supp. II 2002). Radio communications are included in “electronic surveillance” when “both the sender and all intended recipients are located within the United States.” 50 U.S.C.A. § 1801(f)(3).

The hub of the current controversy, then, is the subpart of the FISA definition of “electronic surveillance” that addresses the following situation:

the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes⁵⁸

The warrantless surveillance program involves the acquisition by NSA of the contents of international calls involving a United States person who is within the United States, without issuance of a warrant. FISA allows calls in this category to be intercepted only if they are not “acquired by intentionally targeting” a “particular, known United States person” who is either the sender or an intended recipient of the communication.

Before discussing the legality of the warrantless surveillance included in the current program, it would be useful to describe how NSA has traditionally dealt with international electronic communications that include information about a United States person. General Hayden’s testimony in 2000 before the House Permanent Select Committee on Intelligence is highly illuminating on this issue:

There are other circumstances envisaged by the legislation, by the FISA act, that from time to time we will unintentionally acquire information to, from or about U.S. persons. . . . Under the statute, I may retain and disseminate information unintentionally acquired to, from or about American persons only if the information is necessary to understand or assess foreign intelligence information. What do we need [sic] by “to or from” American persons? I’ll give you an example there. We’ve got someone outside the United States speaking a

58. 50 U.S.C.A. § 1801(f)(1).

foreign language, engaged in a terrorist plot, terrorist activities, and only later in subsequent conversations do we find revealed in such conversations that that person has an American identity – he carries an American passport or she has an American green card. This is information incidentally unintentionally acquired about an American person. The information acquired up to that point can be used in accordance with the FISA statute if it is necessary to understand or assess foreign intelligence information. I cannot continue to target that person without going through the processes I’ve described to you earlier.⁵⁹

General Hayden described a communication involving a United States person outside the United States. No FISA warrant would be required even if the United States person were within the United States, unless the interception targeted the United States person. Let us focus on calls somehow selected by NSA for interception overseas on a basis other than participation in the call of a United States person who is within the United States. Perhaps calls are made from Afghanistan, and NSA is intercepting all electronic communications between the United States and Afghanistan. Calls may be made from a phone number in Afghanistan known to be used by terrorists, and therefore targeted by NSA. It may be the time, or duration, or the subject matter of the calls that leads to their interception, and that focuses NSA’s attention on a United States person within the United States. There is no problem with the initial interceptions, since we are assuming they were not acquired by intentionally targeting the United States person.

Can the United States person who is now of interest be added to a watch list or dictionary so that any future international calls to or from him will be intercepted? The answer is “no,” since taking that step would be intentionally targeting a United States person within the United States. Of course, that would not really be a problem under the facts described by General Hayden, even for a United States person within the United States, since the contents of the calls already intercepted would clearly establish that the United States person is an agent of a foreign power. Thus, the FISC would

59. *Hayden 2000 House Testimony*, *supra* note 30. Earlier in his testimony, General Hayden had described the FISA warrant process. *See also supra* note 55 (discussing the treatment of United States persons who are outside the United States).

unquestionably grant a warrant upon request, permitting complete coverage of the target's international and domestic electronic communications.⁶⁰

What about use and retention of the communications already intercepted, particularly if the situation is not a clear-cut one in which the government will obtain a FISA warrant? As described by General Hayden, NSA has quite elaborate procedures designed to minimize the intrusion on the privacy interests of United States persons as to whom information is incidentally acquired by NSA.⁶¹ Under most circumstances, the identity of a United States person will be deleted from the intelligence reports circulated by NSA, with the name replaced by "U.S. Person." However, the protection for privacy is substantially less than it at first appears. If one of the intelligence agencies receiving a report requests the identity, NSA will provide the information if it is determined to be necessary to understand the foreign intelligence information or assess its importance.⁶²

General Hayden stated that "from time to time [NSA] will unintentionally acquire information to, from or about U.S. persons."⁶³ This suggests that unintentional collection of such information about United States persons is not a serious problem, especially in light of NSA's restrictions on the retention and dissemination of the identifying information unless it is needed to understand or assess the intercepted communication. Such an understanding would, however,

60. Once the FISA probable cause standard is met, the government can even get warrants going beyond electronic intercepts, such as for audio or video surveillance or for physical searches.

61. The detailed NSA manual that regulates the collection, processing, retention, and dissemination of electronic communications to, from, or about United States persons has been released to the public, although with significant redactions. NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE, UNITED STATES SIGNAL INTELLIGENCE DIRECTIVE 18, LEGAL COMPLIANCE AND MINIMIZATION PROCEDURES, July 27, 1993 [hereinafter USSID 18], *available at* <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm>. USSID 18 is supplemented by a detailed manual further regulating the handling of information about United States persons. The version that has been released is riddled with deletions. NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE, U.S. IDENTITIES IN SIGINT, March 1994, *available at* <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/16-01.htm>.

62. *See* USSID 18, *supra* note 61, at § 7.2(c); BAMFORD, BODY OF SECRETS, *supra* note 28, at 448 ("Although NSA takes great pains to eliminate the names of U.S. persons in the reports it sends out, any customer (for instance, CIA or DIA) can obtain the names simply by faxing a request to NSA. The request must offer a reason and state that the name 'is necessary to understand the foreign intelligence or assess its importance.'"). *See generally id.* at 441-49.

63. *Hayden 2000 House Testimony*, *supra* note 30.

fail to appreciate the significance of the way in which NSA goes about collecting communications. While some interceptions are narrowly targeted on particular phone numbers or specific individuals, in other instances NSA picks up all or a significant portion of the communications on certain communications channels or in certain locations. For example, under current circumstances it must be assumed that NSA is very aggressive in seeking to acquire international communications going into or coming out of Iran.⁶⁴ Therefore, NSA's processing of the calls inevitably will turn up information about United States persons in the United States (perhaps those with relatives in Iran) who have been involved in or mentioned in communications that were intercepted. NSA has never disclosed how frequent such "unintentional" acquisition of information about United States persons is, and outsiders are not well placed to make a quantitative estimate, but it seems clear that such interceptions are frequent and growing. James Bamford, an acknowledged expert on NSA and the author of two books about the agency, has observed:

The deliberate targeting of Americans is only one issue. The other is what is done when an American – or a citizen of one of the other UKUSA nations – incidentally turns up in the reams of intercepted traffic. This is becoming more and more likely as technology advances. "The networks have collapsed into one another," said one senior NSA official, "and many of our targets are on the same network that we use. It is just 'the network' – the global telecommunications infrastructure."⁶⁵

It turns out that communications that are "unintentionally" or "incidentally" acquired by NSA because they were not targeted may

64. The agency is certainly intercepting communications within Iran as well, but that does not raise issues under FISA, since neither end of the call would involve a United States person in the United States.

65. BAMFORD, *BODY OF SECRETS*, *supra* note 28, at 441-42. Admiral Hayden was interviewed extensively by Bamford in the preparation of the book. Bamford provides one dramatic example of an incident in which interception not targeted at a United States person nonetheless produced highly personal information about him. "In 1980, while intercepting everything in and out of Libya, NSA analysts discovered that President Jimmy Carter's brother Billy was doing business with and acting as an unregistered agent of the Libyan government." *Id.* at 443.

constitute a very significant proportion of the communications that are intercepted:

A large volume of information flowing through the same signal increases the likelihood that incidental information will be collected. In addition, the fact that many different types of communications flow over the same media results in increased incidental interceptions unrelated to the target of the surveillance. Modern communication satellites are capable of carrying various forms of communication, including television, telephone, and data. Governmental communications often travel over the same signals as private communications, creating a situation in which an innocent man's telephone call to his wife can be transmitted over the same signal as a report from the Chinese embassy to Beijing. Given these developments in the field of COMINT collection and communication technology, this exception for incidentally acquired information threatens to swallow the entire rule.⁶⁶

IV. How Does the Warrantless Surveillance Program Handle “Unintentionally” Collected Information About United States Persons?

The warrantless surveillance program appears to significantly expand the interception of international electronic communications involving United States persons by taking “unintentionally” intercepted communications to, from, or about an individual, and using them as a basis for targeting future communications involving that person.⁶⁷ As discussed above, General Hayden's original

66. Sloan, *supra* note 28, at 1503-04. For a definition of Comint, see *supra* note 30. Although the focus on governmental communications may be less intense now than it was prior to 9/11, as terrorist groups like al Qaeda have become more urgent targets, the point that Sloan is making remains valid. The same circuits that carry the communications of al Qaeda adherents in Afghanistan or Pakistan also carry communications from many other individuals and organizations. If NSA chooses to intercept the entire stream of communications over the circuit, in order to make sure that the al Qaeda messages being sought are captured, then the large volume of messages involving others are considered incidentally intercepted.

67. Since the operational details of the program have not been disclosed, it is possible that it goes further. Thus, the United States persons whose international calls are targeted by NSA may include not only those who send, receive, or are mentioned in intercepted

scenario, in which interceptions not targeted on a United States person provided convincing evidence that he is an agent of a foreign power, presents no challenge. In that case, the government could use the intercepted communications to obtain a FISA warrant covering all electronic communications to or from that person. But what if a suspected terrorist in Pakistan calls a United States person in the United States, the call is intercepted and analyzed upon criteria that have nothing to do with the United States person, and upon examination its contents appear completely innocuous? Analysts might feel that the very fact that the suspected terrorist called the United States person raises suspicions about the United States person, perhaps even strong ones. This situation, however, would probably not be enough to secure issuance of a FISA warrant, since the apparently innocuous phone call would not provide probable cause to believe that the United States person is an agent of a foreign power. What if a second communication (assuming once again that it is intercepted without targeting the United States person) passes between the two individuals? An active dialogue between the suspected terrorist and the U.S. person, even if the contents of the communications appear innocent, might well at some point provide the probable cause needed for issuance of a FISA warrant, but it would not necessarily be easy to say when the tipping point would be reached.

The information that is publicly available strongly suggests that these are the types of situations in which the Administration's surveillance program calls for targeting the United States person without a warrant. The Administration has stated that what it labels the Terrorist Surveillance Program "is narrowly tailored to target only communications where one party is outside the United States and there are reasonable grounds to believe that at least one party is a member or agent of al Qaeda or an affiliated terrorist organization."⁶⁸ Of course in any such a situation it would be possible to seek a FISA warrant, but the essence of the program is the decision to forgo that approach in favor of warrantless surveillance. The

international communications involving someone connected to al Qaeda, but may extend as well to those who are in contact with those who have been in touch with someone connected to al Qaeda. *See generally* Seymour M. Hersh, *Listening In*, NEW YORKER, May 29, 2006, at 25 (describing the use of the technique of "chaining" to identify additional individuals who are considered to be of interest, based on their contacts with others who have already come to the attention of NSA).

68. DOJ Responses to House Judiciary Committee, *supra* note 1, *Responses to Questions from Chairman Sensenbrenner*, at 7.

Administration has not been entirely clear in explaining why it considers the FISA process inadequate, but two possibilities readily suggest themselves: (1) Under the program, NSA is using a standard for probable cause that is easier to meet than the one that would be applied by the FISC; or (2) The same standard is being used for probable cause, but the resources needed to prepare applications, along with the delays and risks of using the formal FISA process, are considered unacceptable.

The probable cause standard being used in the program, and the significance of any delays that would result if FISA were used, will be discussed below. However, before proceeding to address those issues it is worthwhile to summarize the apparent differences between the current warrantless surveillance program and the NSA intercept programs that were in place before 9/11. As described above, FISA does not flatly prevent NSA from intercepting, processing, analyzing, and distributing international communications by, from, or about United States persons in the United States. Many such communications may come to the agency's attention as it intercepts broad categories of communications, or because United States persons are in contact with suspected terrorists overseas. There are some limits on the retention and distribution of such unintentionally acquired information about United States persons, but the information can be used if it is needed to help analysts understand the communications. When interception takes place outside the United States, FISA regulates the *targeting* of communications to or from a particular United States person in the United States.⁶⁹ That requires a FISA warrant based on probable cause. What concerns the agency is that without targeting the suspected United States person it will not acquire all international communications that are potentially relevant, only those that are intercepted using some criterion or criteria other than the identity of the United States person. The warrantless

69. FISA requires a warrant before international electronic communications of United States persons within the United States are targeted. What is often overlooked is that a warrant is not required when those communications are acquired overseas through interception that targets someone else. For example, Judge Richard A. Posner recently analyzed a hypothetical in which a suspected terrorist in a foreign country is calling someone in the United States. Richard A. Posner, *Wire Trap: What if Wiretapping Works?*, NEW REPUBLIC, Feb. 6, 2006, at 15. Judge Posner states that a warrant is needed if "the party on the U.S. side of the conversation is a 'U.S. person.'" To the contrary, no warrant is needed if the target of the interception is the suspected terrorist overseas, or if the acquisition is done on any basis other than "by intentionally targeting" a United States person. Thus, as described *supra* in the text accompanying notes 47-66, FISA is not as restrictive as is sometimes assumed.

surveillance program is based on the fear that some relevant communications may slip through the cracks, in a situation in which the government either cannot get a FISA warrant or is unwilling to do so. Warrantless surveillance may also be an easier and cheaper way to screen possible terrorists than using other investigative techniques.

When the government makes the choice between getting a FISA warrant or choosing not to do so, it does so in the shadow of FISA's criminal sanction: "A person is guilty of an offense if he intentionally . . . engages in electronic surveillance under color of law except as authorized by statute" ⁷⁰ Title III dovetails with FISA by imposing criminal liability on one who, except "as otherwise specifically provided" in Title III:

intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication ⁷¹

Finally, Title III provides:

. . . [the] procedures in this chapter ⁷² or chapter 121 ⁷³ and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted. ⁷⁴

The argument up to this point has established that the warrantless surveillance program involves "electronic surveillance" regulated by FISA because international calls of United States persons within the United States "are acquired by intentionally

70. 50 U.S.C. § 1809(a)(1) (2000). A violation "is punishable by a fine of not more than \$10,000 or imprisonment for not more than five years, or both." *Id.* at § 1809(c).

71. 18 U.S.C.A. § 2511(1)(a) (2000 & Supp. 2006). In most situations, violations may be punished by a prison term of up to five years. *Id.* at § 2511(4)(a).

72. The reference is to Title III, which has been codified as Chapter 119 of Title 18 of the United States Code.

73. The reference is to Chapter 121 of Title 18 of the United States Code, 18 U.S.C.A. §§ 2701-2712 (2000 & Supp. 2006), which addresses issues relating to the disclosure of the contents of electronic communications that have been stored on an electronic communications system.

74. 18 U.S.C.A. § 2511(2)(f) (2000 & Supp. 2006).

targeting” those United States persons.⁷⁵ Neither of the relevant mechanisms for obtaining warrants – under FISA for electronic surveillance or under Title III for all electronic communications – has been utilized. Further, the statutory language quoted above makes it clear that in the absence of a warrant such electronic surveillance is a crime unless it is “authorized by statute.” Therefore, the warrantless surveillance program violates the applicable statutes, and the interceptions being carried out are federal crimes.

The Administration has somewhat indirectly confirmed that its program does indeed fail to comply with the procedures set out in FISA, although it has apparently never explicitly confirmed that the problem arises specifically from the “targeting” of the communications of United States persons. Even in recognizing the conflict between the warrantless surveillance program and FISA, the Administration has not exactly conceded that it has departed from the FISA procedures:

[W]e note that the [Justice] Department’s legal analysis assumes, solely for purposes of that analysis, that the targeted interception of international communications authorized under the Terrorist Surveillance Program would constitute “electronic surveillance” as defined by FISA. As noted in our January 19th paper, we cannot confirm whether that is actually the case without disclosing sensitive classified information.⁷⁶

Despite the caution displayed by the Justice Department’s formulation, no doubt remains about the departure from FISA’s procedures, and the use of the word “targeted” may also tend to confirm that the fundamental legal difficulty with the program is that it *targets* United States persons whose international communications would otherwise be subject to interception only on the basis of some other criterion or criteria.

Of course the Administration, even though forced to acknowledge the existence of the warrantless surveillance program

75. 50 U.S.C.A. § 1801(f)(1) (2003 & Supp. 2005).

76. DOJ Responses to House Judiciary Committee, *supra* note 1, *Responses to Questions from Chairman Sensenbrenner*, at 12; *see id.*, *Responses to Joint Questions from House Judiciary Minority Members*, at 10 (identical wording, except that the definition of electronic surveillance is described as being “in” FISA). The legal analysis that the quote refers to is that presented in the DOJ memorandum that is cited *supra* note 3.

and unable to reconcile it with FISA's procedures, has in no way conceded that the program is illegal, and in fact it has mounted an aggressive defense. The two theories upon which the Administration attempts to bring the program into line with FISA are these:

- The warrantless surveillance program was "authorized by statute" when Congress passed the Authorization for the Use of Military Force ("AUMF") shortly after 9/11.
- If the AUMF is not accepted as authorizing the program, it is unconstitutional for FISA to prohibit the warrantless surveillance program, since this intrudes on the inherent constitutional authority of the President.

This is not the occasion to undertake a detailed analysis of the constitutional issues raised by these defenses of the warrantless surveillance program. Indeed, it may well be that a satisfactory and complete analysis of those issues must await the disclosure of additional information about the program and the way in which it is being carried out. However, even a preliminary analysis of these arguments demonstrates that they provide very slender reeds to support the program.

V. The AUMF Does Not Authorize the Warrantless Surveillance Program

Congress passed the Authorization for the Use of Military Force (the "AUMF") on September 14, 2001, and it became law when President Bush signed it on September 18, 2001.⁷⁷ The legislation authorized the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" of September 11, 2001, or those who harbored those responsible for the attacks. In testimony before the Senate Judiciary Committee, Attorney General Alberto Gonzales stated that the AUMF "is the kind of congressional action the FISA law anticipated."⁷⁸

77. Pub. L. No. 107-40, 115 Stat. 224 (2001).

78. *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the Senate Judiciary Committee*, February 6, 2006 (morning session) (Lexis, News Library) [hereinafter *Feb. 6, 2006 Judiciary Committee Hearing*] (testimony of Attorney General Gonzales).

The Administration sees the current dispute as essentially a rerun of *Hamdi v. Rumsfeld*,⁷⁹ the case involving a man who had been born in the United States (and thus was a U.S. citizen), though his parents had returned to their native Saudi Arabia with Hamdi while he was still a young boy. Late in 2001, he was seized in Afghanistan by the Northern Alliance, a coalition of military groups aligned with the United States in its fight against the Taliban, and he ended up a prisoner of the United States. He was labeled an enemy combatant based on his alleged training with the Taliban, service in a Taliban unit which continued after September 11, 2001, and possession of an assault rifle while in the field with his Taliban unit.⁸⁰ The Supreme Court ultimately remanded the case for further proceedings designed to provide Hamdi an opportunity, in compliance with due process requirements, to dispute the government's allegations. Even before reaching the due process issues, the Court needed to decide if holding Hamdi in the first place violated a statute that provides that no citizen may be imprisoned or detained by the United States "except pursuant to an Act of Congress."⁸¹ The Court divided 5-4 on that issue, with the majority holding that the detention of enemy combatants is an incident of waging war, since it serves the purpose of preventing those who have been captured from returning to the field and taking up arms again.⁸²

United States armed forces fighting the Taliban in Afghanistan, as ordered into battle by the President pursuant to the authority given him by the AUMF, unquestionably had the right to capture and hold enemy fighters. It turned out that Hamdi was a citizen of the United States, but there "is no bar to this Nation's holding one of its own citizens as an enemy combatant."⁸³ The disposition of *Hamdi* provides scant support for the proposition that the AUMF is a statute authorizing warrantless surveillance that is otherwise prohibited by FISA. The 1971 statute on which Hamdi relied was designed to guard against a repetition of the type of mass internment such as that

79. 542 U.S. 507 (2004).

80. *Hamdi*, 542 U.S. at 512-13 (plurality opinion of Justice O'Connor). The government's allegations on these points were supported by a declaration of Michael Mobbs, an official of the Department of Defense.

81. *Hamdi*, 542 U.S. at 517 (O'Connor, J.) (discussing 18 U.S.C. § 4001(a)).

82. *Id.* at 518 (O'Connor, J.). The four Justices joining in Justice O'Connor's plurality opinion were joined, on this issue, by Justice Thomas. *Id.* at 579, 586-87.

83. *Id.* at 519 (O'Connor, J.). The plurality noted that one of the Nazi saboteurs claimed to be a citizen of the United States. *Ex parte Quirin*, 317 U.S. 1, 20 (1942).

imposed on those of Japanese descent during World War II.⁸⁴ The Supreme Court rejected the contention that the statute should be allowed to deprive the President of one of the core aspects of successfully fighting an enemy – preventing captured opponents from being allowed to return to the fight after being captured.

FISA comprehensively and precisely regulates NSA efforts to intercept international communications of United States persons who are in the United States. It states explicitly that warrantless electronic surveillance is illegal unless authorized by statute, yet at no time in the legislative process that led to the AUMF was there the slightest hint that the operation of FISA would in any way be affected. One of the companion cases to *Hamdi*, *Rumsfeld v. Padilla*,⁸⁵ had the potential to shed some light on whether the AUMF should be interpreted to limit earlier statutes having nothing to do with the combat operations conducted under authority of the AUMF. Padilla, a citizen of the United States, had been taken into custody inside the United States, and held in military custody. The United States Court of Appeals for the Second Circuit rejected the government's argument that the AUMF authorized this detention, but the Supreme Court held that Padilla's habeas corpus petition had been filed in the wrong district. When the case was refiled, the Court of Appeals for the Fourth Circuit upheld the government's AUMF argument, but that case too was diverted when the United States transferred Padilla to civilian custody for trial rather than defending in the Supreme Court the holding that the AUMF granted authority for continued military detention.

It would be extraordinary if the precisely-crafted FISA framework, which has been explicitly amended by Congress five times since 9/11,⁸⁶ could silently be altered in the way that the Administration contends, particularly since the AUMF was adopted without there being any reference to NSA, to its mission, to the targeted interception of international communications of United States persons within the United States, or to any aspect of FISA.

84. *Hamdi*, 542 U.S. at 517 (O'Connor, J.).

85. 542 U.S. 426 (2004). The litigation was revived in the Fourth Circuit, and the Supreme Court ultimately denied certiorari. *Padilla v. Hanft*, 126 S. Ct. 1649 (2006), *denying cert. in* 423 F.3d 386 (4th Cir. 2005).

86. *Feb. 6, 2006 Judiciary Committee Hearing* (Sen. Leahy), *supra* note 78.

VI. Recognition of the Fact That FISA Prohibits the Warrantless Surveillance Program Does Not Make FISA Unconstitutional

Perhaps the most creative, but least well defined, arguments advanced in support of the warrantless surveillance program are those suggesting that if FISA prohibits the program the statute itself must be unconstitutional as an impairment of the President's "inherent constitutional authority" under Article II of the Constitution. The invocation of the President's inherent constitutional authority has become something of a mantra for the Administration, and the felicitous phrase is repeated again and again, yet there are almost no developed principles of constitutional law that establish what those powers are or how they are affected by legislation passed by Congress. The reference to "inherent" powers is itself somewhat misleading, since the arguments in support of the warrantless surveillance program are grounded in the text of the Constitution, especially the very first sentence in Article II, which vests the "executive Power" in the President, and the Commander-in-Chief provision. Of course, there are a number of other parts of the constitutional text that are not helpful in defending the program, and therefore are rarely cited by the Administration. The President "shall take Care that the Laws be faithfully executed"⁸⁷ and Congress is granted broad legislative powers over the military, over commerce (which includes telecommunications), and over the public purse.

The brass-knuckles argument vigorously advanced by the Administration is that if FISA prohibits NSA from the warrantless targeting of international communications of United States persons in the United States for interception, then the statute is unconstitutional. There does not appear to be any precedent even vaguely on point – that is, where Congress legislated in an area within its legislative authority and it was nonetheless held by the Supreme Court that the President had inherent authority to act contrary to the statute. The *possibility* that such a situation could arise cannot be dismissed altogether, since a statute that is unconstitutional may properly be declared void by the Supreme Court, but the White House in effect urges adoption of a new and entirely unprecedented principle that would declare unconstitutional all legislation that

87. U.S. CONST. art. II, § 3.

prevents the President from doing anything he considers useful in defending the country.

The celebrated *Steel Seizure Case*⁸⁸ is the precedent most nearly on point, and it offers no support at all for the proposition that FISA is unconstitutional if it in any way inhibits the President's freedom of action as Commander in Chief. In the midst of the bruising Korean War, President Truman feared that an impending nationwide strike in the steel industry would prevent the nation from producing the armaments needed to sustain the military. Therefore, he ordered the Secretary of Commerce to take control of the steel mills in order to assure that production of the vital material would continue. In that case, Congress had never passed a statute forbidding seizure of productive resources, although it had failed to pass legislation that would have granted the President the power to make such seizures. The President was no doubt sincere in his belief that a strike would seriously undermine the war effort, but the Supreme Court held the seizure unconstitutional.

Perhaps most pertinently for present purposes, not only did the result in *Steel Seizure* go against the power claimed by the President, but the influential concurring opinion of Justice Jackson articulated a method for approaching situations in which the Executive's actions deal with the same matters as those on which Congress could act. "When the President acts pursuant to an express or implied authorization of Congress his authority is at its maximum, for it includes all that he possesses in his own right plus all that Congress can delegate."⁸⁹ That principle would be applicable if the AUMF authorized the warrantless surveillance program, but for the reasons discussed above that is a most improbable interpretation of the AUMF. Justice Jackson's second category, which addresses the situation where "the President acts in absence of either a congressional grant or denial of authority,"⁹⁰ is not alleged by anyone to control the present controversy. Justice Jackson's third category, the one to which he consigned President Truman's steel seizure itself, is this:

When the President takes measures incompatible with the expressed or implied will of Congress, his power is at its lowest ebb, for then he can rely only upon his own

88. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952).

89. *Id.* at 635 (Jackson, J., concurring in the judgment and opinion of the Court).

90. *Id.* at 637 (Jackson, J.).

constitutional powers minus any constitutional powers of Congress over the matter. Courts can sustain exclusive Presidential control in such a case only by disabling the Congress from acting upon the subject. Presidential claim to a power at once so conclusive and preclusive must be scrutinized with caution, for what is at stake is the equilibrium established by our constitutional system.⁹¹

The President, Attorney General Gonzales, General Hayden, and others defending the warrantless surveillance program have repeatedly stated that the President considers the program a desirable and effective one that makes it easier for him to prosecute the fight against al Qaeda successfully. However, even if those highly debated assertions are assumed to be true, they do not come close to establishing that the President's Article II powers are being violated simply because the legislative choice made by Congress prevents him from acting in exactly the manner that he prefers. Congress unquestionably has broad powers that are applicable, since it can regulate the interstate and foreign communications industry under the commerce clause, and also regulate the military. Even Attorney General Gonzales has conceded as much:

Well, the fact that the president . . . may have inherent authority doesn't mean that Congress has no authority in a particular area. And we look at the words of the Constitution and there are clear grants of authority to the Congress in time of war. And so if you're talking about competing constitutional interests, that's when you get into sort of the third part of the Jackson analysis.⁹²

The claimed "inherent constitutional authority" that would permit a President to act contrary to a statute whenever he feels that it is necessary to do so in order to successfully prosecute a war, or to defend the country against attack or subversion from abroad, or to conduct the foreign relations of the United States, could not easily be cabined by any defensible limiting principle. Perhaps seeing the need for there to be limits in order to make the theory more palatable,

91. *Id.* at 637-38 (Jackson, J.) (footnote omitted).

92. *Feb. 6, 2006 Judiciary Committee Hearing* (afternoon session) (testimony of Attorney General Gonzales), *supra* note 78.

President Bush has stated that assassination would be impermissible: “I don’t think a president can order the assassination of a leader of another country with which we’re not at war. There are clear red lines.”⁹³ While assassination would be reprehensible, it is difficult to see why it would necessarily be illegal if the warrantless surveillance program is not. FISA prohibits the surveillance program, but there is no statute that prohibits assassinations.⁹⁴ Thus, for purposes of a *Steel Seizure* analysis along the lines suggested by Justice Jackson, assassination would not be in the third category (as the current FISA controversy is), but rather in one of the first two categories. The Administration has placed great emphasis on intelligence collection as a traditional aspect of warfare and national defense, but surely assassination of enemy leaders and agents is similarly intertwined with the history of warfare and international conflict. If the unformed constitutional theory advanced by the Administration were to be accepted, judicial supervision of its boundaries would be difficult if not impossible. In practical terms, the President would have secured the “blank check” that the *Hamdi* Court withheld.⁹⁵

Application of the theory of claimed “inherent constitutional authority” to the facts of the warrantless surveillance program cannot proceed much further without a lot more information about the nature and implementation of the program. However, I see no realistic possibility that the facts, once known, will lead to the conclusion that the President’s constitutional authority is being usurped.⁹⁶ Since the Administration is claiming, in essence, that the President cannot function effectively as Commander in Chief without the ability to bypass the FISC on surveillance of certain international communications, it would need to make a detailed case that has not yet been made (at least in public) – that the need to get warrants in the situations covered by the program has a dramatic effect on his

93. Eric Lichtblau & Adam Liptak, *Bush and His Senior Aides Press On in Legal Defense for Wiretapping Program*, N.Y. TIMES, Jan. 28, 2006, at A13.

94. After the Church Committee exposed CIA assassination plots, there was consideration of legislation to prohibit assassination. “However, President Ford headed off such legislation by adopting” an executive order “prohibiting U.S. employees from engaging in ‘political assassination.’” STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 373 (3d ed. 2002). The current prohibition remains part of an executive order rather than a statute. See Executive Order 12,333, *supra* note 55, at § 2.11.

95. *Hamdi*, 542 U.S. 507, 536 (2004) (plurality opinion of Justice O’Connor) (“a state of war is not a blank check for the President when it comes to the rights of the Nation’s citizens”).

96. See, e.g., *Morrison v. Olson*, 487 U.S. 654 (1988) (upholding the statute that substantially restricted presidential ability to remove an independent counsel).

ability to perform as Commander in Chief. If the case were made, there is no reason to predict that the potential constitutional collision between Article II and FISA, as predicted by the Administration, would actually take place. Congress built a number of safety valves into FISA as originally written,⁹⁷ and it has repeatedly amended the statute to meet the Administration's concerns after 9/11. Rather than identifying changes that it claims need to be made in FISA, either on constitutional or policy grounds, the Administration has chosen instead, in secret, to act contrary to the statute.

Not enough is publicly known about the program to permit a full exploration of the constitutional assertions being made by the Administration. There are dramatic inconsistencies pervading the various assertions being made about the program, and many of the most important facts have not yet been disclosed to the public. One critical unknown is the size of the program. The original *New York Times* article disclosing the existence of the program reported that officials familiar with it had said that NSA was eavesdropping on "up to 500 people in the United States at any given time."⁹⁸ More recently, Seymour Hersh wrote that a government consultant told him "that tens of thousands of Americans had had their calls monitored in one way or the other."⁹⁹ The magnitude of the program,

97. When Congress declares war, warrantless electronic surveillance is permitted for 15 days. 50 U.S.C. § 1811 (2000). In an emergency, electronic surveillance may be instituted immediately, so long as an application for a FISA warrant is filed within 72 hours. *Id.* at § 1805(f). A major concern expressed by the Administration about the 72-hour provision, in addition to its brevity and the fact that it is only available when the FISA probable cause standard is expected to be met, is that if emergency interception begins and no FISA warrant is issued, the target might then be notified. *Feb. 6, 2006 Judiciary Committee Hearing, supra* note 78 (afternoon session) (testimony of Attorney General Gonzales) (if an order is not obtained, "the presumption is that the judge will then notify the target of that surveillance during that 72-hour period").

98. Risen & Lichtblau, *supra* note 1; see Barton Gellman, Dafna Linzer & Carol D. Leonnig, *Surveillance Net Yields Few Suspects; NSA's Hunt for Terrorists Scrutinizes Thousands of Americans, but Most Are Later Cleared*, WASH. POST, Feb. 5, 2006, at A1 ("Two knowledgeable sources placed [the number of Americans who have had their conversations recorded or their e-mails read without warrants] in the thousands; one of them, more specific, said about 5,000.").

99. Hersh, *supra* note 67, at 25. The important ambiguity in the reported statement is whether the monitoring being described involves the contents of the communications, which implicates FISA, or whether only transactional information is being acquired. See generally CONGRESSIONAL RESEARCH SERVICE, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: LEGAL BACKGROUND AND RECENT AMENDMENTS (2006); Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215*, 1 J. NAT'L SECURITY L. & POL'Y 37 (2005).

which the Administration has so far refused to reveal, has significant implications for a number of the other arguments being advanced in support of the program.

One recurrent theme advanced in support of the program is that the standard of “probable cause” being used by NSA in carrying out the program is the same standard as that used by the FISC. If true, this assertion may help to blunt concerns being raised about entirely innocent individuals having their communications intercepted.¹⁰⁰ However, if the total number of United States persons being targeted in the United States has increased dramatically, that would strongly suggest that a lower standard of probable cause is being used. The Administration has been careful in most instances to state that “a” probable cause standard is being used, often buttressed by a citation to the recent Supreme Court decision in *Maryland v. Pringle*¹⁰¹ that is designed to show that it does not take very much information to establish probable cause.¹⁰² It is far from clear that *Pringle*, properly understood, supports the low threshold of suspicion that the Administration claims is sufficient. The case involved arrests made when three men all were in a car stopped for speeding at 3:15 a.m. The driver consented to a search of the vehicle, which led to the discovery of a roll of money and five baggies containing cocaine. None of the men would say who owned the drugs and the money, so the police arrested all three. *Pringle* later admitted that the cocaine was his, but challenged the legality of the arrest. The Court concluded that “there was probable cause to believe *Pringle* committed the crime of possession of cocaine, either solely or jointly,” since “it was reasonable for the officer to infer a common enterprise among the three men.”¹⁰³

Although the government repeatedly cites *Pringle* as reflecting the appropriate standard of probable cause, one of the cases distinguished by the Supreme Court’s decision in *Pringle* may more closely resemble the circumstances of United States persons who

100. Even if the standards were established to be the same, the core concerns of the Fourth Amendment would remain a serious obstacle to upholding the legality of the program, since the critical determination on probable cause is made by an NSA employee rather than by a detached and neutral magistrate. “The Fourth Amendment contemplates a prior judicial judgment.” *Keith*, *supra* note 10, 407 U.S. at 317.

101. 540 U.S. 366 (2003).

102. See, e.g., DOJ Responses to House Judiciary Committee, *supra* note 1, *Responses to Questions from Chairman Sensenbrenner*, at 30 (the “‘reasonable grounds to believe’ standard is a ‘probable cause’ standard of proof, see *Maryland v. Pringle*”).

103. *Pringle*, 540 U.S. at 372-73.

have some contact with an al Qaeda adherent without manifesting membership in or allegiance to the group. In *Ybarra v. Illinois*,¹⁰⁴ police officers had obtained a search warrant authorizing them to search a tavern and its bartender for evidence of drugs. The Court held that the warrant did not permit pat-down searches of the patrons who were in the bar at the time the warrant was executed, absent individualized suspicion.¹⁰⁵ Thus, to the extent that the program targets United States persons based on ambiguous contacts with suspected al Qaeda members, it seems very likely that the standard of probable cause being applied is not as demanding as the one that would be applied by the FISC.

The government has denied that it is changing the standard of probable cause, arguing that the principal reason for using FISA in the situations within the warrantless surveillance program is that “pursuing ‘prior judicial review by the FISA court’ requires significantly more time.”¹⁰⁶ However, in establishing internal procedures and in allocating resources, the Justice Department and other agencies can exert substantial influence on the speed of the FISA process. Even if administrative changes need to be made in order to allow FISA warrants to be obtained more quickly in some cases, it hardly seems likely that such inconveniences could amount to an intrusion into the President’s sphere sufficient to allow him to triumph in a “category three” case. Justice Jackson’s formulation places presidential power at its lowest ebb when the President acts in violation of a statute. Given that over 2,000 FISA warrants were granted last year,¹⁰⁷ it could not possibly be the case that the need to get another 500 – or even another 1,000 – would be a difficulty of constitutional dimension, even if expedition were needed in some instances. Admittedly, there might be a serious problem if the need arose to get 10,000 warrants a year, but that would provide irrefutable proof that the probable cause standard being applied had been substantially diluted from that used by the FISC. Moreover, Congress has shown itself quite willing to give prompt and sympathetic consideration to any proposed FISA modifications that are shown to be necessary, but the Administration has spurned those overtures.

104. 444 U.S. 85 (1979).

105. *Id.* at 92-93.

106. DOJ Responses to House Judiciary Committee, *supra* note 1, *Responses to Questions from Chairman Sensenbrenner*, at 14; *see id.* at 38-39.

107. *See supra* note 27.

Conclusion

The Administration has been very successful so far in withholding from the public the details of the warrantless surveillance program, making a precise assessment of its legality very difficult to carry out. However, it appears that the core violation being committed is the targeting of international calls involving United States persons in the United States who appear to have had at least some contact with someone connected to al Qaeda, but where it is uncertain that the FISC would find that there is probable cause to believe that the potential target is an agent of a foreign power.

FISA plainly requires a warrant in the situations described. The AUMF cannot plausibly be taken to have provided statutory authorization for warrantless interceptions under these circumstances. Moreover, the “inherent constitutional authority” theory advanced by the Administration flies in the face of the classic *Steel Seizure* formula of Justice Jackson that places the President’s power at its lowest ebb when he acts contrary to a statute. If a President is permitted to violate a comprehensive and long-standing statutory system, without even seeking to obtain desired adjustments from Congress, our system of separation of powers will be altered in ways that are both radical and undesirable.