USA PATRIOT Act, the Fourth Amendment, and Paranoia: Can They Read this While I'm Typing?

Justin F. Kollar

Cite as 3 J. High Tech. L. 67 (2004)

> They that can give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety.[1]
>
> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.[2]

I. INTRODUCTION

We cherish our Fourth Amendment privacy rights during times of peace and security, but they suffer greatly during times of perceived peril.[3] On October 26, 2001, President George W. Bush, himself the son of a wartime president, signed the lugubriously-named USA PATRIOT Act (USAPA) into law.[4] The Act is massive in scope and

---

1. Attributed to Benjamin Franklin.

2. United States. v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 314 (1972) [hereinafter *Keith*] (Powell, J.).

3. *See* Katz v. United States, 389 U.S. 347, 364 (1967) (discussing the long-running Presidential sanctioning of wiretapping in national security cases). S*ee also* John Borland & Lisa Bowman, *Politics: Weighing Security Against Liberties*, CNET News.com, August 27, 2002, *at* http://news.com.com/2009-1001-954565.html. The article quotes Jonathan Zittrain, the co-director of Harvard University Law School's Berkman Center for Internet and Society: "People pretty readily let go of privacy concerns as soon as security is involved." *Id.* Zittrain goes on to note that people will generally choose terrorism as a greater threat than an overly intrusive government. *Id.* The article itself notes that the internet, despite its "libertarian roots," is structured so that massive centralized database logs are commonplace, and that even massive research databases like Lexis-Nexis are working more closely with the Federal Government since September 11th, 2001, providing user-related information. *Id.*

4. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USAPA) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

 ISSN 1536-7983

reach, and has quickly become a flashpoint of controversy in the contemporary civil liberties lexicon.[5] Congress assembled and passed USAPA with a quickness uncharacteristic of the federal government, in a mere six weeks following the unprecedented terrorist attacks of September 11, 2001.[6]

President Bush and his Attorney General, John Ashcroft, awash in a rising tide of public hysteria, succeeded in enacting legislation criticized by many as an attempt to consolidate too much power in the executive branch of the Federal government.[7] Critics rightly recognize that parts of the Act may seriously compromise the Fourth Amendment and the fundamental right of privacy by expanding the ability of executive branch law enforcement agencies to conduct electronic surveillance and wiretapping on suspected criminals.[8] The USAPA furthers this objective by using ex parte proceedings in secret courts exercising a greatly reduced standard of review over surveillance applications made by the Attorney General.[9] The term "Patriot Act" is now shorthand for a growing polarization in American politics, and has already raised serious questions concerning abuses by those it newly empowers.[10]

5. *See, e.g., Ashcroft Defends USA Patriot Act*, REUTERS, July 21, 2003, http://www.dailyweb.info/forums/showthread.php?t=215&goto=nextnewest (highlighting the growing debate over USAPA's reach). The Republican-led state legislature in Alaska passed a resolution condemning USAPA. *Id.* John Ashcroft is quoted in the article: "We use these tools to secure the liberties of our citizens. We use these tools to save innocent lives." *Id.* The Attorney General also blamed the public's negative perception of USAPA on erroneous and incomplete media portrayal of the legislation. *Id.*

6. *See, e.g.*, John Podesta, *USA Patriot Act, The Good, the Bad and the Sunset,* HUMAN RIGHTS, Winter, 2002, *at* http://www.abanet.org/irr/hr/winter02/podesta.html (describing the provisions of USAPA relating to electronic surveillance as a "sound effort" notwithstanding the haste of the laws passage).

7. *See* Timothy Lynch, Policy Analysis #443, *Breaking the Vicious Cycle: Preserving our Liberties While Fighting Terrorism*, Cato Institute, June 26, 2002 at 8 (on file with author). The author discusses generally the dilution of warrant requirements and probable cause requirements, citing Yick Wo v. Hopkins, 118 U.S. 356 (1886), and Johnson v. United States, 333 U.S. 10 (1948), among others, in support of the proposition. *Id.* The article sets forth an overview of what the author perceives to be an agenda of expanded law enforcement power attributed to the Bush administration. *Id.*

8. *Id.*

9. *Id.*

10. *See infra* note 16 and accompanying text (describing the alleged abuses committed under USAPA as reported by the Department of Justice's Inspector General). *See, e.g.*, Philip Shenon, *Report on USA Patriot Act Alleges Civil Rights Violations*, N.Y. TIMES, July 21, 2003, at A1. A recent report by the US Inspector General presented to Congress in July, 2003, and heavily commented on by national media, accuses the Justice Department of abusing its new powers in

USAPA effectively gives the Attorney General the power to conduct electronic surveillance over almost anybody alleged to bear any tenuous connection to a group that advocates violence.[11] Civil libertarians accuse the President and Attorney General of making a power grab, asserting that the USAPA violates Fourth Amendment privacy safeguards.[12] While certain provisions are very intrusive, the Act and its subsequent reading by the Foreign Intelligence Surveillance Court of Review does reflect the historic tendency of the judiciary to defer to the Executive, in cyberspace or otherwise, particularly during wartime.[13]

What troubles many about the Act is the perceived marginalizing of the judiciary and the relaxing of the standards to be met by prosecutors seeking to gather evidence.[14] Civil libertarians point to

dozens of instances. *Id.* Many of the abuses complained of occurred in the Bureau of Prisons, the department having custody of most of the immigrants rounded up in the months following September 11, 2001. *Id.* In one frightening instance a federal prison doctor allegedly told an inmate that if "I was in charge, I would execute every one of you." *Id. See infra* note 16 and accompanying text (describing the alleged abuses committed under USAPA as reported by the Department of Justice's Inspector General).

11. *See* Curt Anderson, *Appeals Panel Rejects Secret Court's Limitations on Terrorist Wiretaps*, ASSOCIATED PRESS, Nov. 18, 2002, *at* http://www.boston.com/news/daily/18/111802_spy_court.htm (discussing the decision of the Foreign Intelligence Surveillance Court of Review to reject certain restrictions on electronic surveillance as violative of USAPA).

12. *See* Robin Mejia, *More Surveillance on the Way*, THE NATION, November 11, 2002, *at* http://www.thenation.com/doc.mhtml?i=20021111&s=mejia20021030&c=1. Mejia discusses letters from the Attorney General's office that describe "anecdotal" evidence that ISPs have begun to freely turn over records to law enforcement officers without warrants. *Id.* The article describes USAPA as the first step in a program of civil liberty reductions, in conjunction with the pending Cyber Security Enhancement Act (CSEA), in itself an interesting piece of legislation which would further reduce the protection of electronic records. *Id.* The CSEA provides that ISPs could turn over records upon belief that the disclosure would prevent some future danger. *Id.* Further, the need for a reasonable belief that the disclosure is related to the prevention of the danger is reduced to a simple requirement that the ISP be acting in "good faith.." *Id.*

13. *See, e.g.*, In re: Sealed Case 02-001, 310 F.3d 717, 722-725 (D.C. Cir. 2002) [hereinafter *Sealed Case*], *infra* notes 136-144 and accompanying text (describing the deference accorded to the executive in matters of national security).

14. *See* Muslim Comm. Assoc. v. Ashcroft, C.A. No. 03-72913 (E.D. Mich. filed July 30, 2003). The lawsuit challenges the constitutionality of Section 215 of the Act, which permits, according to the Plaintiffs, prosecutors to gather evidence of people not suspected of criminal activity. *Id.* at ¶ 1. *See also* Electronic Privacy and Information Center, *The USA PATRIOT Act*, *at* http://www.epic.org/privacy/terrorism/usapatriot/ (providing a concise overview of USAPA's impact on the evidence gathering provisions of both the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510 *et. seq.* (2000 & Supp. 2002), and the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801 *et*

the Supreme Court's own jurisprudence in highlighting the fact that the intersection of free speech and law enforcement is particularly volatile.[15] USAPA so quickly changed the American political landscape that it is difficult to prospectively assess its impact, although some argue the Act is simply a manifestation of the cyclical expansions and contractions of civil liberties not unusual in American history.[16]

A historical analysis of the Fourth Amendment provides this context, specifically in regard to the warrant requirement for electronic surveillance.[17] Prior to USAPA, the level of judicial oversight required for any particular intelligence-gathering endeavor hinged on whether the intelligence sought was "foreign intelligence" or a more straightforward criminal investigation.[18] Where this semantic line is drawn determines the necessity, or lack thereof, for a warrant.[19] This distinction determines who will grant the authority

seq. (2000 & Supp. 2003).

15. *See, e.g.*, Mitchell v. Forsyth, 472 U.S. 511, 522-23 (1985) (granting Attorney General qualified immunity from suit in case concerning warrantless wiretapping in national security case). The Court in this case stated: "National security tasks are carried out in secret. . . [u]nder such circumstances, it is far more likely that actual abuses will go uncovered then that fancied abuses will give rise to unfounded and burdensome litigation." 472 U.S. at 522. The Court also relied heavily on *Keith* for the proposition that national security cases propounded unique fusions of first and fourth amendment concerns and notes that the government even when acting with benign motives is likely to abuse its power under such a vague notion as that of "national security." 472 U.S. at 523 (citing *Keith*, 407 U.S. at 313-14).

16. *See* U.S. DEPT. OF JUSTICE OFFICER OF THE INSPECTOR GENERAL, REPORT TO CONGRESS ON IMPLEMENTATION OF SECTION 1001 OF THE USA PATRIOT ACT, July 17, 2003, http://www.usdoj.gov/oig/special/03-07/index.htm. The Department of Justice Inspector General's Office reports 34 of what it describes to be credible Patriot Act complaints, of a total 1,073 reported complaints allegedly invoking the Patriot Act. *Id.* at 6. The Inspector General reports opening only six new Patriot Act-related investigations, continuing eight and closing three investigations. *Id.* at 7. Of the remaining claims, it referred twenty-eight to internal affairs offices within the Department of Justice and forwarded two to the FBI. *Id.* at 11. The same report reviews the treatment of the 762 aliens detained in the post-September 11 time period. *Id.* at 12.

17. *See, e.g.*, *How the USA PATRIOT Act puts the CIA back in the Business of Spying on Americans, at* http://www.aclu.org/congress/1102301j.html. [hereinafter *ACLU Statement*] (discussing historical reasons for restrictions on CIA's domestic surveillance activities).

18. *See* United States v. Truong Dinh Hung, 629 F.2d 908, 913-14 (4th Cir. 1980) (allowing admission of evidence gathered under reasonable warrantless searches, but disallowing evidence gathered after the primary purpose of the investigation became criminal in nature).

19. *See* Sealed Case, 310 F.3d at 722-25 (illustrating the waning distinction between foreign intelligence surveillance and ordinary criminal surveillance activities for purposes of Constitutional analysis).

for the surveillance, and USAPA redraws its boundaries in dramatic fashion.[20] Analysis of Fourth Amendment history, and its bearing on issues of electronic surveillance and national security, elicits a better understanding of the changes USAPA works on contemporary privacy interests.[21] This paper discusses the origin and evolution of the Fourth Amendment's protections against warrantless wiretapping, and includes a selective overview of various portions of USAPA affecting those protections.

II. THE FOURTH AMENDMENT & THE AMERICAN RIGHT TO PRIVACY

The Fourth Amendment to the U.S. Constitution reads:

> 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.[22]

The framers of the Constitution did not envision modern telecommunications, and thus the Fourth Amendment on its face seems to limit a protected area of a purely physical nature.[23] While the founding fathers could not have envisioned the degree to which high-tech terrorists in the twenty-first century could instill fear, they deliberately created a living document based on simple principles that is capable of dealing with almost any set of circumstances.[24]

Historically, and as a result of this Constitutional elasticity, whenever national security is threatened, privacy protections are accordingly reduced.[25] Serious threats result in public hysteria and a

20. *Id.*

21. *Id.* (discussing the historical evolution of the warrant requirement in foreign intelligence surveillance cases).

22. U.S. CONST. amend. IV. *See also Muslim Comm. Assoc.*, discussed *supra* at note 14.

23. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (discussing the evolution of Fourth Amendment concerns). That Court summarized the original character of Fourth Amendment inquiry, as embodied by the *Olmstead* holding. *See infra* notes 32, 62-63 and accompanying text (discussing the *Olmstead* case). The Court characterized the original mode of inquiry as encompassing a primarily physical realm, while noting that contemporary inquiry focused on the person and not the place. *Katz*, 389 U.S. at 351. Justice White would not have read the case to affect cases of national security. *Id.* at 363. Justice Black's dissent points out the impossibility of the Constitution's drafters having foreseen the tapping of telephone wires as such technology was fantastic at the time. *Id.* at 365.

24. *See Katz*¸ 389 U.S. at 365. Justice Black's dissent attempts at some length to apply the Fourth Amendment as originally intended to the facts at hand, acknowledging that the Fourth Amendment was to be given a "liberal construction." *Id.*

25. *See, e.g.*, Secretary of Transportation Norman Mineta, Mineta Sees Acts of

consequent pressure on the executive to act in a manner the public perceives as strong and decisive.[26] The courts are charged to read the Constitution as tolerant of these intermittent and limited intrusions into civil liberties.[27] In the period just after September 11th 2001, in keeping with historical trends, an unsettled public willingly placed greater power in the hands of receptive federal law enforcement agencies.[28] Despite the dire nature of the circumstances, many erstwhile statesmen and others criticized USAPA for its breadth and dramatic scope, positing that by diminishing judicial oversight, reducing operational barriers and widening the scope of what is searchable, the Act abrogates the Fourth Amendment.[29]

The Fourth Amendment right to privacy is rooted in the English common law, as is most of our revered Constitutional jurisprudence.[30] The need for protection against unlawful search and seizure arose out of colonial frustration with the British occupiers' arbitrary imposition

Friendship Toward Arab-Americans and Muslims, Remarks at University of Rochester Annual Meliora Weekend, October 12, 2001, *at* http://usinfo.state.gov/usa/civilrights/mineta.htm (describing how Presidents throughout history have abrogated civil liberties in the name of protecting national security, and citing the internment of Japanese-Americans during the Second World War as egregious examples).

26. *See id.*

27. *See* WILLIAM REHNQUIST, ALL THE LAWS BUT ONE, 224-25 (2000) (writing that "[t]here is no reason to think that future wartime presidents will act differently from Lincoln, Wilson, or Roosevelt, or that future Justices of the Supreme Court will decide questions differently from their predecessors. It is neither desirable nor is it remotely likely that civil liberty will occupy as favored a position in wartime as it does in peacetime. But it is both desirable and likely that more careful attention will be paid by the courts to the basis for the government's claims of necessity as a basis for curtailing civil liberty"). The Chief Justice's book is as comprehensive an outline as one would wish to see addressing the question of where to set the balance between civil liberties and order during wartime, addressing Lincoln's suspension of habeas corpus. *Id.* at 11-26. The internment of Japanese-Americans during World War II. *Id.* at 184-203. In addition, the three-year period during which the State of Hawaii was ruled by martial law. *Id.* at 212-18.

28. *See, e.g.,* Nancy Chang, SILENCING POLITICAL DISSENT: POST SEPTEMBER 11 ANTITERRORISM MEASURES THREATEN OUR CIVIL LIBERTIES (2002) (discussing the shift towards greater law enforcement powers). One such willing and receptive Assistant Attorney General, Daniel J. Bryant, of the United States Department of Justice, sent a letter to Senate leaders considering USAPA, openly urging the abrogation of the Fourth Amendment in favor of warrantless searches. *Id.*

29. *See id. See also USA PATRIOT Act Boosts Traditional Government Powers While Cutting Back on Traditional Checks and Balances, at http://www.aclu.org/congress/1110101a.html*. [hereinafter *ACLU Analysis*] (discussing concisely the major concerns of civil libertarians with regards to USAPA's impact on constitutionally protected privacy rights). *Id.*

30. *See, e.g.,* Chimel v. California, 395 U.S. 752, 760-61 (1969) ("The (Fourth) Amendment was in large part a reaction to the general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence.").

of justice.[31] The invention of the telephone and rapid technological improvements occurring in the late nineteenth and early twentieth century raised novel issues of interpretation not seen in the first century or so of American political history and reopened the once-settled question of where to draw the line between public and private.[32]

The Fourth Amendment provides that in the absence of special circumstances, law enforcement must obtain the approval of a neutral judicial officer before any search or seizure happens in a place subject to a reasonable expectation of privacy.[33] Specifically, requests for search warrants must satisfy three conditions.[34] First, the search must be "reasonable" – the courts have long struggled to define the parameters of this reasonableness.[35] Second, the warrant must specify with particularity the subject matter of the search.[36] Finally, a neutral magistrate must be imposed between the law enforcement official and the object of the search.[37]

The test of reasonableness is elastic and requires both a liberal construction and broad application.[38] In each case it requires a balancing of the need for the particular search against the invasion of personal rights that the search entails.[39] Courts must consider the scope of the particular intrusion, the manner in which it occurs, the justification for initiating it, and the place it happens.[40] Therefore, this malleable notion of "reasonableness" lies at the center of a fluid doctrine governing the standards applied by the courts in the areas of search and seizure.[41] This fluid standard of reasonableness permits doctrinal shift.[42]

31. *See id.*
32. *See* United States v. Olmstead, 277 U.S. 438, 466 (1928) (declining to extend to telephone conversation the same Fourth Amendment protection it accorded to sealed envelopes containing letters).
33. Ellsberg v. Mitchell, 709 F.2d 51, 66-68 (D.C. Cir. 1983) (holding that to state a *prima facie* constitutional violation it is not necessary for the plaintiff to prove that the challenged surveillance was acquired unlawfully, rather the burden is on the defendant to show that the evidence was gathered under the 'foreign intelligence' exception).
34. *See Katz*, 389 U.S. at 354-55.
35. *Id.*
36. *Id.*
37. *Id.*
38. Bell v. Wolfish, 441 U.S. 520, 559 (1979) (collecting cases) (describing the test of reasonableness as being "not capable of precise definition or mechanical application").
39. *Id.*
40. *Id.*
41. *Id.*
42. *Id.* at 559.

In our complex society the right to privacy has grown to encompass more than mere property rights.[43] As a result of this shift, which occurred between the industrial revolution and the passage of USAPA, the Fourth Amendment today is more like an umbrella, moving to protect a mobile person, than a roof protecting a house.[44] From 1978 until very recently, analysis of the Fourth Amendment's general prohibition of warrantless wiretapping centered on the dichotomy between surveillance of foreign powers (and their agents) and surveillance of ordinary people for criminal purposes.[45] The timely nature of the threat posed by terrorism to U.S. security interests and continued doctrinal shift in the U.S. Federal Courts has resulted in a move away from Fourth Amendment protections not atypical in a time of war, and there is now emerging an understanding that the use of warrantless electronic surveillance is likely to expand considerably and will be held Constitutional.[46]

III. THE SCOPE OF USAPA IS FAR BEYOND THE TRADITIONAL NOTION OF NATIONAL SECURITY

USAPA consists of 156 individual sections grouped under ten Titles.[47] Title II of the Act is entitled "Enhanced Surveillance Procedures" and contains 25 sections that concern Titles 18 and 50 of the United States Code and Rules 6 and 41 of the Federal Rules of Criminal Procedure.[48] Seven sections of Title II concern the Foreign Intelligence Surveillance Act alone.[49] Most of the Act will "sunset" in five years, but nine of the most contentious of the twenty five

43. *See Katz*, 389 U.S. at 353. "[O]nce it is recognized that the Fourth Amendment protects people and not simply areas – against unreasonable search and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure." *Id*. (quotation marks omitted).

44. *See id*.

45. *See, e.g., Truong*, 629 F.2d at 913-14. *Truong* is now abrogated by the FISC Court of Review decision in *Sealed Case. See infra* notes 136-144. *Cf*. Zweibon v. Mitchell, 516 F.2d 594, 613-14 (D.C. Cir. 1975) (en banc) (containing *dicta* in the plurality opinion suggesting that "absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional."). *See also* discussion *infra* note 18 (discussing circumstances under which courts will admit the fruits of warrantless searches prior to USAPA).

46. *See id.*

47. USAPA, P.L. No. 107-56, 115 Stat. 272 (2001).

48. P.L. 107-56, Title II, § 203(a), 115 Stat. 278 (2001) codified at FED. R. CRIM. P. 6; P.L. 107-56, Title II, § 219, 115 Stat. 291 (2001) codified at FED. R. CRIM. P. 41.

49. P.L. 107-56, Title II, at §§ 206-208, 214, 215, 218, 225 (2001) (codified as amended at 50 U.S.C. § 1801 *et seq.* (2000 & Supp. 2003)).

sections in Title II are exempt and shall not expire.[50]

Many of USAPA's provisions are relatively insipid, like its generic, one-sentence condemnation of religious hatred.[51] USAPA sweeps widely, however, encompassing the esoteric as well.[52] Furthermore, in addition to the electronic surveillance provisions of the Act there is much space devoted to such diverse issues as prevention of money-laundering,[53] border protection,[54] and intelligence sharing.[55] In many respects USAPA indicates the Federal government's desire to modernize its capabilities in sectors not traditionally thought of as security-related.[56] The short span of time elapsing between the events of September 11, and USAPA's subsequent drafting and adoption has been illustrated by some early difficulties in the court system.[57] Interpretations of the Act's more complex issues are sure to result in many years of highly technical litigation encompassing wider-reaching issues.[58]

50. P.L. 107-56, Title II, at §§ 205, 208, 210, 211, 213, 216, 224 (2001). Section 224 is the sunset provision itself, making a full forty percent of the Title II provisions permanent. Section 224 further exempts from the sunset provisions any investigations ongoing at the time of sunset. *Id.* at § 224.

51. USAPA, P.L. 107-56, Title I, § 102 (2001) ("Sense of Congress condemning discrimination against Arab and Muslim Americans").

52. *Id.* at Title III, § 322 ("Corporation represented by a fugitive").

53. *Id.* at Title III ("International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001").

54. *Id.* at Title IV ("Protecting the Border").

55. *Id.* at Titles V ("Removing Obstacles to Investigating Terrorism"), VII ("Increased Information Sharing for Critical Infrastructure Protection") and IX ("Improved Intelligence").

56. *See generally* USAPA, P.L. 107-56, Title III (2001). Banks are scrambling to assemble compliance procedures to deal with the Act's measures, designed to make it more difficult for terror suspects to move money around electronically. *See* Barbara Pickney, *Trustco at Top of List No One Wants to Make*, THE BUSINESS REVIEW, Sept. 27, 2002, *at* http://albany.bizjournals.com/albany/stories/2002/09/30/story1.html. Trustco Bank N.A. has become the first bank cited under USAPA for violating provisions designed to detect and prevent money laundering. *Id.*

57. *See* United States v. Reid, 206 F. Supp. 2d 132, 138-42 (D. Mass. 2002) (citing the Dictionary Act at 1 U.S.C. § 1 *et seq*. (2000), finding that the definition of the term "vehicle" did not include airliners for the purpose of imposing criminal liability). This early embarrassment occurred during the prosecution of a man who attempted to down a transatlantic flight with crude bombs concealed in his sneakers, when Federal prosecutors were forced to drop a count from their indictment based purely on the drafting of one section. *Id. See also* Senate Report No. 107-166, To Clarify the Definition of "Vehicle" for Purposes of Criminal Penalties Relating to Terrorist Attacks and Other Acts of Violence Against Mass Transportation Systems, S. REP. NO. 107-166 (2002).

58. *See id*. (highlighting the unforeseen intricacies of overhauling entire complexes of national security policies and regulations).

IV. A HISTORY OF WARRANTLESS ELECTRONIC SURVEILLANCE.

Many civil libertarians, aware that courts historically look askance at wiretapping, did not learn until recently that the executive branch already enjoys tremendous latitude in the area of foreign-intelligence gathering.[59] Less surprising is the degree to which aggressive law enforcement officials have sought to make use of wiretapping for evidence gathering purposes since the advent of the telecommunications age.[60] The history of electronic surveillance in American jurisprudence turns on a number of discreet issues, small in number but evolving conceptually along with our understanding of communications and technology.[61]

As recently as 1928, a full half-century into the telephone age, the Supreme Court refused to read the Fourth Amendment as offended by a search of any kind other than an actual physical search of a physical premises.[62] In the early case of U.S. v. Olmstead, the Supreme Court explicitly rejected the notion of wiretapping as being an activity offensive to the Fourth Amendment's prohibition of unreasonable search and seizure.[63] This requirement of actual physical invasion is known as the "physical trespass" doctrine.[64]

Civil libertarians may take note that for decades prior to the passage of FISA, Congress imposed no constraints on the executive with regards to gathering any information that fell under the aegis of national security.[65] By 1961, courts started to perceive the "physical

59. *See* Berger v. New York, 388 U.S. 41, 45 (1967) (citing 1862 Cal. Stat., p. 288, CCLXII). As early as 1862 the state of California found it necessary to prohibit the electronic interception of telegraph messages, made possible by the nascent technology known as electricity. *Id.*

60. The *Berger* opinion contains an excellent overview of the history of both eavesdropping and wiretapping through the ages, noting that "this activity has been with us for three-quarters of a century." *Berger*, 388 U.S. at 46.

61. *See, e.g.*, *Sealed Case*, 310 F.3d at 725-26 (discussing the evolution of warrantless wiretapping doctrine).

62. *Olmstead*, 277 U.S. at 466. This was a prohibition-era case leading to a string of cases in which the Court focused on whether or not there had been a physical intrusion onto a premises. *See infra* notes 63-68 and accompanying text (discussing the physical trespass doctrine). In another case the surreptitious recording of conversations was held to be quite acceptable where the microphone was placed against a wall. Goldman v. United States, 316 U.S. 129, 133 (1942). *Accord* On Lee v. United States, 343 U.S. 747, 751-52 (1952).

63. *Olmstead*, 277 U.S. at 466.

64. Silverman v. United States, 365 U.S. 505, 510 (1961) (discussing the "physical trespass" doctrine).

65. *Keith*, 407 U.S. at 310-11. (discussing the ways use of warrantless electronic surveillance had been sanctioned continuously since July of 1946). Herbert Brownell, Attorney General under Eisenhower, was up front about his support for the practice, writing law review articles on the topic). *See also* Herbert Brownell, *The Public Security and Wiretapping*, 39 CORNELL L. REV. 195, 202 (1954).

trespass" doctrine as perhaps too rarefied to be effective or logical.[66] The Supreme Court in *Silverman v. United States* effectively broke the doctrine's back, acknowledging that technology had advanced to a point where it was no longer logical to equate a protected sphere of liberty with a protected physical locus.[67] Here, for the first time the Court acknowledged that the recording of overheard statements may be a Fourth Amendment issue, notwithstanding the lack of physical trespass.[68]

Six years later the Court put yet a finer point on the issue of physical trespass, in considering whether a listening device placed on top of a telephone booth for the purpose of intercepting the conversations occurring within was a search and seizure for Fourth Amendment purposes.[69] Writing with uncharacteristic bluntness, Justice Potter Stewart revisited his opinion from Silverman, writing that "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"[70] The Court in *Katz* acknowledged the moribundity of Olmstead's "physical trespass" doctrine, and envisioned its replacement by a new standard, one recognizing that the Fourth Amendment protected "people, not places."[71] Finally, the Supreme Court imposed the requirement of a search warrant as a prerequisite to the clandestine recording of telephone conversations.[72]

66. *Silverman*, 365 U.S. at 511-12 (Douglas, J. dissenting) (wrestling with the dilemma of how to distinguish equivalent invasions of privacy distinguished by inches, where the placing of a microphone on a surface is permitted but the driving of the microphone into a surface is not permitted). The Court held unconstitutional the making by law enforcement of certain recordings by the driving of a microphone through a party wall and into a heating duct, thus constituting a trespass. *Id. See also Goldman*, discussed *supra* note 62 and accompanying text.

67. *Silverman*, 365 U.S. at 511-12 (discussing the shortcomings of the "physical trespass" doctrine). Justice Stewart considered the historical sanctity of the home as man's refuge, and held the recordings to have been made by physical intrusion into a "constitutionally protected area." *Id.* at 512. The use of this phrase came back to haunt Stewart, as he expressed in *Katz*, "it is true that this court has occasionally described its conclusions in terms of 'constitutionally protected areas,' but we have never suggested that this concept can serve as a talismanic solution to every Fourth Amendment problem." *Katz*, 389 U.S. at 352 (internal citations omitted).

68. *Silverman*, 365 U.S. at 511-12.

69. United States v. Katz, 389 U.S. 347, 349 (1967).

70. *Id.* at 350. The Court further strengthened its decision in *Silverman* by its rejection of the government's reliance on the absence of physical intrusion as being the determinative factor. *Id.*

71. *Id.* at 351. Refreshingly, the Court by 1967 had come to recognize the "vital role that the public telephone has come to play in private communication." *Id.* at 352.

72. *Katz*, 389 U.S. at 356 (acknowledging that the agents had acted with restraint and pointed to the ease with which they could have obtained a warrant for the surveillance). The Court reiterated the need for the interposition of a judicial

The elimination of the physical trespass doctrine importantly erased one of the few bright lines delimiting the area of reasonableness, and broadened the scope of debate to include much more tenuous and ephemeral forms of intrusion.[73] The Court did not wait long to apply this new criteria to the questions raised by nascent wiretapping technology, deciding in the same year the landmark case of *Berger v. New York*.[74]

The *Berger* case centered on a challenge to the particularity and probable cause aspects of New York's extremely permissive wiretap statute.[75] The Court found that the statute violated the Fourth Amendment by authorizing the issuance of warrants upon the simple oath or affirmation of any number of law enforcement officials, ranging from the Attorney General down the chain of command to police sergeants.[76] The authorizing official needed only to affirm the existence of a reasonable belief in the surveillance's likelihood of yielding evidence of a crime.[77] The statute, although it did require a judge to issue the surveillance order, problematically did not specify with sufficient clarity the subject matter or purpose of the search.[78]

Although not a national security case, the *Berger* Court addresses the issue of rapid technological advances outpacing legislative developments, an issue very much at the heart of today's national security problems.[79] The Court noted the breadth of the intrusion on

officer between the citizen and the police. *Id.* at 357 (citing its decision in Wong Sun v. United States, 371 U.S. 471, 481-82 (1963).

73. *Katz*, 389 U.S. at 353 (holding "[t]he fact that the electronic device employed to achieve [the surveillance] did not happen to penetrate the wall of the booth can have no constitutional significance").

74. *Berger*, 388 U.S. at 62-63 (1967). The Court certainly started its analysis from scratch, noting at the outset that "eavesdropping is an ancient practice which at common law was condemned as a nuisance." 388 U.S. at 45 (citing 4 Blackstone, Commentaries 168).

75. *Berger*, 388 U.S. at 62-63. The Supreme Court (Clark, J.) also held that the law violated the Fourth and Fourteenth Amendments, but rejected Fifth and Ninth Amendment challenges. *Berger*, 388 U.S. at 44.

76. *Berger*, 388 U.S. at 55-56. The Court found many problems with the New York law, finding that although the law did impose the neutral magistrate, the failure to provide for any particularization in terms of expected fruit was (among other factors) fatal. *Id*.

77. *Berger*, 388 U.S. at 54. "It permits the issuance of the order, or warrant for eavesdropping, upon the oath of the attorney general, the district attorney or any police officer above the rank of sergeant stating that there is reasonable ground to believe that evidence of crime may be thus obtained." (internal quotes omitted).

78. *Id.* at 55.

79. *Id.* at 46-49 (discussing new technologies and their implications for the Fourth Amendment). Justice Clark attempts to apply this technological drift to the original language of the Fourth Amendment after discussing at length the origins of eavesdropping, wiretapping and the public policy reasons for constraining the use of those techniques. *Id.* at 49. The Court in that case wrote, "the law, though

the Fourth Amendment posed by eavesdropping and determined that the New York statute fell well outside the Constitution's requirements of particularity, because it did not sufficiently tell law enforcement to search or seize particular people, places or things.[80] The statute authorized the use of indiscriminate wiretapping similar in form to the roving wiretaps permitted by USAPA.[81] The *Berger* Court weighed the severity of the intrusion against the nature of the area invaded (a private home), and held the contemplated surveillance, long and continuous in scope, far too severe under the circumstances.[82] The Court drew contrasts between its holdings in this case and in *Osborn*, where the evidence sought directly reflected the commission of a specific offense and the warrant described the precise and discriminate circumstance of the eavesdropping.[83]

Little more than a year later the Court again considered the boundaries of permissible surveillance, this time in a case that did involve national security concerns.[84] The question in the case concerned the standard a District Court ought to use when evaluating the legality of evidence obtained through possibly illegal surveillance.[85] In that case, federal prosecutors accused a Soviet emigre of conspiring to transmit information to the Soviet Union pertaining to the national security of the United States.[86] The Court granted certiorari to resolve the question of whether the prosecution needed to turn over the records of the challenged surveillance to the trial judge for a limited, *in camera* inspection, or allow a more public examination including the defense.[87]

The Court, in *Butenko*, acknowledged that under *Katz*, it should read the Fourth Amendment to protect a person's private conversations as well as his private premises.[88] This harmonized with

jealous of individual privacy, has not kept pace with these advances in scientific knowledge." *Id.*

80. *Berger*, 388 U.S. at 55. This failure of particularization results in a failure of probable cause for the warrant, in that no "man of reasonable caution [would] believe an offense has been or is being committed." 388 U.S. at 55.

81. *Berger*, 388 U.S. at 58.

82. *Id.* at 58-62. The Court ultimately concluded that "we cannot forgive the requirements of the Fourth Amendment in the name of law enforcement. *Id.* at 62-63.

83. 388 U.S. at 64, (Douglas, J. concurring) (citing Osborn v. United States, 385 U.S. 323, 349-54 (1966)). Douglas was pleased to be finally overruling *Olmstead* and bringing electronic surveillance within the purview of the Fourth Amendment. *Id*.

84. Alderman v. United States, 394 U.S. 165 (1969) [hereinafter *Butenko*].

85. *Id.* at 167.

86. *Id.* at 169.

87. *Id.* at 170.

88. *Butenko*, 394 U.S. at 178.

the Court's holding in *Silverman*, recognizing that the unlawful nature of the home invasion formed the basis for excluding the evidence.[89] The federal prosecutors in *Silverman*, sounding a now-familiar refrain, argued that the evidence concerned matters of national security too delicate for argument in open court.[90] The Court overruled these claims, ordering the District Court to openly determine whether the evidence offended the Fourth Amendment and whether such a violation reflected upon the petitioner's conviction.[91] If the District Court determined that the evidence tainted the conviction, it would order a new trial.[92] The *Butenko* case struck an important blow against government efforts to shroud in secrecy the circumstances by which the U.S. government conducted surveillance.[93]

Shortly thereafter, in 1972, the U.S. Supreme Court decided the landmark case of *United States v. United States District Court* (the *Keith* case).[94] The Court here announced a significant boundary, refusing to extend the nascent "foreign intelligence exception" to include the warrantless surveillance of domestic persons in ordinary criminal investigations.[95] In *Keith*, prosecutors relied on warrantless electronic surveillance of an individual suspected of planning terrorist attacks on government offices.[96] Attorney General Mitchell approved the challenged wiretaps without judicial approval, relying on the power of the President to act in defense of national security, as exercised through the Attorney General.[97]

89. *Id.*
90. *Id.* at 181.
91. *Id.* at 186.
92. *Id.*
93. *Butenko*, 394 U.S. at 183 (noting that "adversary proceedings are a major aspect of our system of criminal justice," and that particularly where the inquiry is intensely factual it is necessary to preserve the adversarial nature of the proceedings).
94. *Keith*, *supra* note 2, at 297 (quoting Justice Powell).
95. *Id.* (permitting warrantless surveillance where the primary purpose of the investigation was to gather intelligence relating to the activities of a foreign power or its agents but requiring a warrant under almost all circumstances to spy upon citizens in ordinary criminal matters). Powell's reasoning resounds still today, although provisions of the PATRIOT Act echo the opinion of *Keith*. *See* 407 U.S. at 321 (stating that "we [the Court] do [not] think the Government's domestic surveillance powers will be impaired to any significant degree. A prior warrant establishes presumptive validity of the surveillance and will minimize the burden of justification in post-surveillance judicial review"). 407 U.S. at 321.
96. *Id.* at 300.
97. *Id.* at 301. The Attorney General submitted an affidavit and a sealed exhibit containing the logs of the surveillance. *Id.* The government proffered several justifications for the surveillance, all of which the Court rejected; first, that judicial review would obstruct the President; second, that the subject of the intelligence was

The *Keith* Court acknowledged, as the Court continues to, this Constitutional power of the President to obtain foreign intelligence information, but refused to allow the executive branch to assert this power to seek intelligence information not concerning the actions of a foreign power or its agents.[98] More than a quarter century later, the courts still regarded Keith as clearly establishing the necessity of a warrant for domestic security intelligence gathering, notwithstanding that the Court in that case declined to address issues "which may be involved with respect to activities of foreign powers or their agents."[99] The *Keith* Court actually ducked the foreign intelligence issue.[100] Nonetheless, Circuit courts applying *Keith* in ensuing years started to recognize the existence of the "foreign intelligence" exception to the warrant requirement for searches occurring within the U.S.[101]

The last major pre-FISA case to address the foreign intelligence exception to the warrant requirement was *United States. v. Truong Dinh Hung*.[102] In that case the Attorney General authorized the surveillance of a citizen thought to be transmitting sensitive information to the government of North Vietnam.[103] The *Truong* Court reinforced the "primary purpose" test, holding that prosecutors could use certain types of warrantless evidence so long as their primary purpose in gathering the evidence was foreign intelligence

not relative to a primarily criminal investigation; third, that courts would not have the expertise to determine whether probable cause existed; and finally, the federal government argued that disclosure to a judge of information regarding the search would create national security hazards. *Id.* at 318-19.

98. *Keith*, 407 U.S. at 302-05 (interpreting the statute as merely disclaiming an intent to limit any power the President possessed under the Constitution). Justice Powell's opinion read the Government's challenge as being an opportunity to answer a "question left open by *Katz*: "whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security. . ." *Id*. at 309, quoting *Katz*, *supra* note 23, at 358, n. 23.

99. United States v. Bin Laden, 126 F. Supp. 2d 264, 271 (S.D.N.Y. 2000) (extending reach of 'foreign intelligence' exception to include search of American citizen's home in foreign country).

100. *Keith*, 407 U.S. at 321-22. (declaring "[w]e 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.").

101. *Bin Laden*, 126 F. Supp. 2d at 271 (citing United States v. Clay, 430 F.2d 165, 171 (5th Cir. 1970), and United States v. Butenko, 494 F.2d 593, 605 (3d Cir. 1974) in upholding warrantless foreign intelligence surveillance.) *Id.*

102. *See* discussion *supra* note 18 and accompanying text.

103. 629 F.2d 908 (4th Cir. 1980). The Foreign Intelligence Surveillance Court of Review in 2002 upbraided other circuit courts for following the "primary purpose" test as set forth in *Truong*. *Sealed Case*, 310 F.3d at 725.

surveillance.[104] The Court, however, still subordinated these foreign policy concerns partially to larger Fourth Amendment issues, and declined again to further extend the 'foreign intelligence' exception.[105]

V. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

The Foreign Intelligence Surveillance Act (FISA) of 1978[106] is the often-litigated statute that authorizes the Executive branch to conduct electronic surveillance and physical searches for foreign intelligence purposes without a warrant.[107] It effectively codified the "foreign intelligence exception" to the warrant requirement and established a secret court system (the FISC, or Foreign Intelligence Surveillance Court) to consider wiretap and surveillance requests made by Federal prosecutors.[108]

Congress passed FISA to bring to an end the nationwide disparity in the interpretation of various Supreme Court decisions relating to national security-related intelligence gathering.[109] As noted in the *Bin Laden* decision, the Circuit Court cases developing the foreign intelligence exception predated FISA.[110] While FISA governs the surveillance of agents of foreign powers, it is Title III, of the Omnibus Crime Control and Safe Streets Act of 1968 (OCCSA) that protects U.S. citizens, requiring that law enforcement officers obtain a traditional search warrant before undertaking surveillance.[111] This

104. *Truong*, 629 F.2d at 914 (deferring to the necessity of the executive being able to manage an effective and efficient foreign policy).

105. *Id.* at 915 (limiting foreign intelligence exception to instances where the "interests of the executive are paramount").

106. *See generally* The Foreign Intelligence and Surveillance Act (FISA) of 1978, codified at 50 U.S.C. § 1801 *et seq*. (2000 & Supp. 2003).

107. *See infra* notes 113-17 (discussing FISA in-depth). The statute originally did not provide for physical searches, this was achieved by amendment in 1994. Pub L. No. 103-359, 108 Stat. 3444 (1994), codified as amended at 50 U.S.C. §§ 1821-1829 (2000) (concerning physical searches). The court in United States v. Nicholson had no problem upholding these provisions, holding that the physical search was not subject to more stringent requirements than the electronic surveillance. United States v. Nicholson, 955 F. Supp. 588 (4th Cir. 1997) (holding that "Defendant's argument that physical searches are per se more intrusive than electronic surveillance is unavailing in light of *Katz*"). 955 F. Supp at 591.

108. P.L. 107-56, Title II, § 208, 115 Stat. 283 (2001) (codified as amended at 50 U.S.C. § 1803 (2000 & Supp. 2001)) (describing the powers, procedures and duties of the Foreign Intelligence Surveillance Court and the FISC Court of Review).

109. *See* ACLU v. Barr, 952 F.2d 457, 460-61 (D.C. Cir. 1991) (discussing purposes of FISA).

110. 126 F. Supp. 2d at 272, at n. 8.

111. Omnibus Crime Control and Safe Streets Act (OCCSSA) of 1968, codified as amended at 42 U.S.C. § 3711 *et seq.* (2000).

emergent and important dichotomy required the observance of a much higher procedural standard for non-foreign intelligence surveillance targets.[112]

When Congress enacted FISA in 1978, it increased the President's power, acting through the Attorney General and the Justice Department, to gather foreign intelligence information by electronic means.[113] FISA describes how foreign intelligence surveillance is to occur in the United States.[114] FISA also brings a degree of clarity to the conflicted area at the intersection of the President's foreign affairs power and the Constitutional ban on unreasonable search and seizure.[115] The act explicitly provides the power to conduct electronic surveillance targeting a foreign power or the agent of a foreign power.[116] FISA's definition of "foreign power" includes not only foreign governments, but also terrorist organizations, foreign national factions, or foreign based political groups comprised of primarily non-U.S. persons.[117] Furthermore, FISA provides for a Foreign Intelligence Surveillance Court, to hear the surveillance applications made by federal law enforcement officials.[118] The proceedings of this

112. *Id.* Parties seeking to conduct surveillance of U.S. persons under this standard must satisfy the traditional requirements of probable cause. *Id.*

113. *See* The Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. 95-511, 92 Stat. 1783, codified as amended at 50 U.S.C. §§ 1801 *et seq.* (2000 & Supp. 2003).

114. P.L. 107-56, Title X, § 1003, 115 Stat. 392 (2001), codified as amended at 50 U.S.C. §§ 1801(f)(1-4) (Supp. 2001); P.L. 107-56, Title II, § 208, 115 Stat. 283 (2001), codified as amended at 50 U.S.C. § 1803(a) (2000 & Supp. 2001) ("Designation of Judges"). *See also* 50 U.S.C. § 1821(5) (2000 & Supp. 2001) (defining the term "physical search"); 50 U.S.C. § 1822(c) (2003) ("Authorization of physical searches for foreign intelligence purposes").

115. *See Bin Laden* for a discussion of this conflict. 126 F. Supp. 2d at 272-73

116. P.L. 107-56, Title X, § 1003, 115 Stat. 392 (2001), codified as amended at 50 U.S.C. §§ 1801 (b)(1-2)(Supp. 2001). The surveillance must be intended to acquire foreign intelligence information. *Id.*

117. 50 U.S.C. § 1801(a) (2000 & Supp. 2001). The full definition reads: (a) "Foreign power" means— (1) a foreign government or any component thereof whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments." *Id.*

118. P.L. 107-56, Title II, § 218, 115 Stat. 291 (2001), codified as amended at 50 U.S.C. §§ 1803 (2000 & Supp. 2001) (describing the Court's makeup) and 1804(a) (2000 & Supp. 2001) ("Applications for Court Orders," describing the procedures followed by the attorney general when applying for a warrant). The court consists of seven district court justices appointed by the Chief Justice of the U.S. Supreme Court. 50 U.S.C. § 1803(a) (2000 & Supp. 2001). The Court will apply a minimal

court are necessarily secret, and a party seeking to challenge the validity of the surveillance can do no more than submit the request that the court conduct an *in camera*, ex-parte review of the surveillance application.[119] Although there is a Court of Review from the FISC, it heard not a single appeal from 1978 until 2002.[120]

In 1995, President Clinton acted to erect informational barriers among law enforcement agencies, intending to prevent the pollution of criminal investigations with evidence gathered by warrantless electronic surveillance and vice versa.[121] By 1997, Circuit Courts interpreting FISA regarded it as "reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens."[122]

VI. USAPA DRAMATICALLY EXPANDS FISA POWERS OF THE PRESIDENT

Frequent litigation left little doubt as to FISA's constitutionality as of September 11, 2001.[123] At the time of USAPA's passage, federal law provided for four basic categories of electronic surveillance: orders to intercept communications; search warrants; trap and trace orders; and subpoenas.[124] USAPA makes it easier to use FISA to gather information from all these categories.[125] Although USAPA

level of scrutiny to the surveillance authorization requests. *See* United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984), discussed *infra* at note 122.

119. P.L. 107-56, Title V, § 504(a), 115 Stat. 364 (2001), codified as amended at 50 U.S.C. § 1806(b) (2000 & Supp. 2002) ("Use of information").

120. *Sealed Case*, 310 F.3d at 719.

121. Exec. Order 12949 (Feb. 9, 1995).

122. *Nicholson*, 955 F. Supp. at 590. (citing *Keith*, 407 U.S. at 327). The court in *Nicholson* noted the Second Circuit's decision in *Duggan* (also applying the reasonableness test). 955 F. Supp. at 591.

123. *See Duggan*, 743 F.2d 59, 72 (2d Cir. 1984) (upholding presidential power to engage in warrantless surveillance to collect foreign intelligence information). The Second Circuit held that compelling concerns of national security justified disparate treatment of U.S. citizens and non-resident aliens under FISA. 743 F.2d at 72. The court further held that surveillance taken for national security purposes may be used against defendants (in this case members of the Irish Republican Army) in a criminal action as well. *Id.* The case also highlights the minimal scrutiny afforded to alienage distinctions in cases of this type. 743 F.2d at 76. *Accord* United States v. Megahey, 553 F.Supp. 1180, 1186 (E.D.N.Y. 1982) (companion case, reiterating that "[t]here is no universal requirement of a warrant before a search can be conducted under the fourth amendment.").

124. *See Electronic Frontier Foundation Analysis of the Provisions of the USA PATRIOT Act*, at 4 (on file with author) [hereinafter *EFF Analysis*]. A trap and trace order authorizes the collection of telephone numbers dialed to and from a particular machine, but not the actual communications themselves. *Id*. *See also* 18 U.S.C. §§ 3121-3127 (2000 & Supp. 2003) (setting forth the statutory exceptions to the prohibition on pen registers and trap-and-trace orders).

125. *See id*.

affects at least 15 federal statutes, it most substantially alters FISA.[126] Besides modifying foreign intelligence procedures, USAPA relaxes the level of protection afforded certain types of electronically stored information traditionally considered sensitive or personal, and provides inter alia for the sharing of educational statistics with the FBI.[127]

Section 218 of USAPA significantly modifies FISA, doing away with the "primary purpose" test and replacing it with a "significant purpose" test.[128] The gathering of foreign intelligence no longer need be the primary thrust of the surveillance, but need only be a significant factor.[129] Even more striking, Section 206 provides authority for the FISC to grant so-called "roving wiretaps" not specific to a particular jurisdiction, telephone number or email address but which can cross jurisdictional boundaries.[130] This wide latitude effectively permits the surveillance of much otherwise lawful activity, giving rise to Constitutional concerns of overbreadth and vagueness.[131]

126. *See* FISA, 50 U.S.C. § 180 *et seq*. (2000 & Supp. 2003).

127. *See ACLU Analysis*, discussed *supra* at note 29. The ACLU is troubled by the provisions in USAPA which make it easier for law enforcement to access the vast caches of student data maintained by educational institutions as part of the National Education Statistics Act of 1994. Pub. L. No. 103-382, Title IV, 108 Stat. 4029 (1994), codified at 20 U.S.C. §§ 9001-9009, since repealed entirely by P.L. 107-279, Title IV, § 403(1), 116 Stat. 1985 (2002), codified as amended at 20 U.S.C. § 9561 *et seq*. (Supp. 2002). *Id. See also infra* note 165 (discussing § 507 of USAPA).

128. P.L. 107-56, Title II, § 218 (2001), codified as amended at 50 U.S.C. § 1804(a)(7)(B) (2000 & Supp. 2001). One may note that the FISC had rejected only one warrant application since its inception, even under the older standard. *Sealed Case*, *supra* note 119, at 717-18. *See also* 50 U.S.C. § 1804(b) (2000 & Supp. 2001) (describing the Court of Review). While this fact may make the distinction between primary-purpose and significant purpose seem superficial, it is one the executive branch, the legislature and the judiciary all saw fit to erase after the terrorist attacks of September 11, 2001. USAPA, P.L. 107-56, Title II, § 218 (2001); *Sealed Case*, 310 F.3d at 728.

129. P.L. 107-56, Title II, § 218 (2001). S*ee also Sealed Case*, 310 F.3d at 728 (discussing the evolution of the primary-purpose test as being a function of judicial misreading of FISA and misplaced reliance on the *Truong* case).

130. P.L. 107-56, Title II, § 206 (2001), codified as amended at 50 U.S.C. § 1805 (c)(2)(B) (2000 & Supp. 2002). USAPA made FISA's roving wiretap provisions akin to those found in 18 U.S.C. § 2510 *et seq*. (2000 & Supp. 2002) (governing domestic surveillance). *See also Commentary of the National Institute for Trial Advocacy*, Title 50 NITA 36 (2003).

131. *See ACLU Analysis, supra* note 29 (alleging that even membership in a mainstream group like PETA (People for the Ethical Treatment of Animals, a large group that includes a faction prone to acts of petty vandalism) might be grounds for deportation of non-citizens under USAPA).

VII. USA PATRIOT ACT AND THE KONOP CASE

Another court construed and upheld Section 209 of USAPA.[132] Section 209, amending the Wiretap Act to eliminate "storage" from the definition of "wire communication," seriously vexes many civil libertarians.[133] By clarifying the distinction between a stored communication and one in transit, USAPA makes it easier for law enforcement officials to gain access to stored and unopened email and voicemail messages.[134] Illustrating the significance of this change, the progressive Ninth Circuit Court of Appeals held that a secure website located on a server is not in transmission but in storage, and thus the unauthorized viewing by the defendant's employer did not offend the Wiretap Act.[135]

VIII. THE FISC COURT OF REVIEW DECISION OF 2002

Importantly, the U.S. Foreign Intelligence Court of Review recently heard its first appeal since the 1978 passage of FISA, and its decision struck a decisive blow for the Bush-Ashcroft view of the post 9/11 civil liberties landscape.[136] Interestingly, procedural issues may prevent the issue from ever reaching the United States Supreme Court.[137] In *In Re: Sealed Case 02-001*, a three-judge panel

132. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002). A disgruntled airline pilot maintained a secure website where employees who had a login and password could view bulletins critical of their employer. *Id.* A vice-president using another employee's login information viewed the website and the pilot was suspended. *Id.*

133. *See EFF Analysis*, *supra* note 124, at 6-7. (discussing the ways in which getting a search warrant is easier than getting an intercept order. To get an intercept order under Title III it is necessary to make a showing that probable cause is present that the target of the intercept order has committed one of a list of enumerated serious crimes. Intercept orders require the law enforcement official to report back to the court and are only good for 30 days. Search warrants require only probable cause). *Id.*

134. *Id. See also* H.R. REP. 107-236(I) (2001) (showing Congress' awareness of the narrowness of the courts definition of intercept, and desire to make the definition apply to voice mail messages). *Id.* The court in *Konop* notes that stored communications are less-protected than communications in transit and under USAPA voicemail and websites now enjoy far less protection from surveillance than in the past. *Konop*, 302 F.3d 868.

135. 302 F.3d 868, 876. The court applied a narrow definition of the term "intercept" – as "acquisition contemporaneous with transmission" in accord with the intent of the Wiretap Act. *Id. See* 18 U.S.C. § 2511(1)(a) (2000 & Supp. 2002).

136. *In re: Sealed Case 02-001*, 310 F.3d 717, 722-25 (D.C. Cir. 2002). (granting the application for surveillance as originally sought, rejecting restrictions imposed by FISC Court). *Id.*

137. *Id.* One notes however that the three judges on the Court of Review are appointed by the Chief Justice of the U.S. Supreme Court (presently William

considered certain restrictions imposed by FISC upon a surveillance request it had granted.[138] By invalidating the restrictions, the Court of Appeal addressed the long-standing separation of law enforcement and intelligence functions, holding no basis for its continued observance.[139]

Citing legislative history, the Court of Review held that FISA never intended to exclude use of FISA surveillance for criminal prosecution, and faulted Circuit Courts for relying on *Truong* (a pre-FISA case), *Megahey*, and other cases in applying the "primary purpose" test.[140] The court astonishingly held USAPA's explicit abrogation of "primary purpose" as the ratification of a nullity.[141] The court did not stop at that, but continued to admonish the FISC court, noting that even its certification of purpose required under FISA was better judged by the Attorney General's articulation and not by the FISC court's inquiry.[142] The court then construed its own new construction of FISA, and held that it did not offend the Fourth Amendment.[143] The court concluded by implying that reliance on the faulty Truong doctrine may have resulted in the failure to anticipate the September 11, 2001 attacks.[144]

IX. USAPA CREATES DRAMATIC NEW LAW-ENFORCEMENT POWERS.

Section 802 of USAPA also defines a new crime of "domestic terrorism," which could include activities of many American protest groups that now engage in conduct arguably "dangerous to human

Rehnquist). 50 U.S.C. § 1803(b) (2000 & Supp. 2001). Further, in *ex parte* proceedings (the Federal Government is the only party) the Court of Review is free to raise issues not before the original FISC court. 310 F.3d 717 at n. 6.

138. 310 F.3d 717. The panel consisted of Senior Circuit Judge Guy (who wrote the court's opinion), and Senior Circuit Judges Silberman and Leavy. *Id.* The court ordered that the law enforcement officials and intelligence officials not share the proceeds of the surveillance, and that the Justice Department be subjected to chaperoning procedures. *Id.* at 720.

139. *Id.* at 724-25. Not only did the court do away with the distinction, but it professed bewilderment as to how it had ever come to be read into FISA. *Id.* (discussing the inextricability of criminal and intelligence investigations from one another).

140. *Sealed Case*, 310 F.3d at 724 (citing H.R. REP. NO. 95-1283, at 49 (1978)). The court found similar intent in the Senate Report on FISA. *Id.* (citing S.REP. NO. 95-701, at 10-11) (1978)). The court also discussed the evolution of the primary purpose test, noting that no decision had tied the test to any statutory language. *Id.*

141. *Id.* at 735 ("even though. . .the original FISA did not contemplate the "false dichotomy, the PATRIOT Act actually did, which makes it no longer false.") *Id.*

142. *Sealed Case*, 310 F.3d at 736.

143. *Id.* at 746.

144. *Sealed Case*, 310 F.3d at 746 (noting the high degree to which the criminal process is integrated into the process of fighting terrorism).

life."[145] USAPA significantly expands law enforcement powers in the domestic arena in areas not confined to foreign intelligence gathering.[146] Section 209 permits law enforcement to acquire stored wire communications like voicemail with a search warrant instead of an intercept order.[147]

Sections 219 ("Single jurisdiction search warrants for terrorism") and 220 ("Nationwide service of search warrants for electronic evidence") of the Act provide for the issuance of search warrants in a single jurisdiction that extend beyond the reach of that jurisdiction.[148] These warrants may issue in one jurisdiction and serve on an internet service provider anywhere in the country, with no requirement that it specifically name that provider.[149] Section 213 further relaxes notification requirements attaching to search warrants, permitting law enforcement officers to "sneak and peek," notifying the subject of the warrant in a "reasonable period" instead of immediately, where the immediate notification of the subject would have "an adverse result."[150]

USAPA permits expanded use of trap and trace orders, altering the statutes to include email and electronic communications, as well as

145. P.L. 107-56, Title VIII, § 802(a), 115 Stat. 376 (2001), codified as amended at 18 U.S.C. § 2331(5)(A-B)(i-iii) (2000 & Supp. 2001) (stating in relevant part: "The term 'domestic terrorism' means activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping."). The ACLU has noted that this new definition would permit the deportation of non-citizen WTO protestors and other political activists associated with organizations promoting civil disobedience. *ACLU Analysis*, *supra* notes 123-24 (discussing the possible breadth of interpretation logically attributable to the new definitions set forth in USAPA).

146. *See EFF Analysis*, *supra* note 124, at 7-8 (summarizing the other impacted areas of law enforcement).

147. *See Konop*, 302 F.3d at 868 (discussing the implications of the new definition of "stored communications).

148. P.L. 107-56, Title II, § 219, 115 Stat. 289 (2001), codified at FED.R. CRIM. P. 41(a). S*ee also* 18 U.S.C. § 2703 (2000 & Supp. 2002). These roving search warrants require only that an activity relating to terrorism has occurred in the jurisdiction issuing the warrant. *Id.*

149. P.L. 107-56, Title II, §§ 209(2), 210, 212(b)(1), 220(a)(1), 220(b), 115 Stat. 283, 285, 291, 292 (2001), codified as amended at 18 U.S.C. § 2703 (2000 & Supp. 2002) ("Required disclosure of customer communications or records").

150. P.L. 107-56, Title II, § 213 (2001) ("Authority for delaying notice off the execution of a warrant"). The court must find reasonable cause that the immediate notice of the warrant's execution will have an adverse result. *Id.* The language of the section further provides that the court may amend the warrant to extend the period for the giving of notice "for good cause shown." *Id.*

software processes and devices.[151] Courts authorizing these pen registers can enter ex-parte orders authorizing their use anywhere nationwide under the now-familiar standard of relevance to ongoing criminal investigation.[152]

Section 210 of USAPA alters the Electronic Communications Privacy Act.[153] The change permits law enforcement access to more types of information including payment information like a bank account or credit card number, IP addresses, and session duration.[154] USAPA also facilitates the sharing of information between law enforcement agencies and branches of the judiciary, without regard as to whether the information was gathered under FISA or Title III.[155] This troubles civil libertarians who note that FISA explicitly places information gathering in the hands of the Department of Justice as a reaction to widespread illegal surveillance of U.S. citizens by both the CIA and NSA during the 1970's.[156]

Section 203(a) of USAPA substantively modifies Rule 6 of the Federal Rules of Criminal Procedure, authorizing the disclosure of grand jury information to intelligence services.[157] The section also provides for disclosure to law enforcement any foreign intelligence information whether or not concerning a U.S. person relating to the ability of the U.S. to protect against actual or potential attack.[158] Section 203(b) also allows law enforcement officials to provide the

151. 18 U.S.C. § 3121 (2000 & Supp. 2001), as amended by P.L. 107-56, Title II, § 216(a), 115 Stat. 288 (2001) ("Modification of authorities relating to use of pen registers and trap and trace devices"). This provision of USAPA does not sunset. P.L. 107-56, Title II, § 216 (2001).

152. *See* 18 U.S.C. § 3121 (2000 & Supp. 2001).

153. P.L. 107-56, Title II, § 210 (2001).

154. *Id.* (illustrating the amendments to the Electronic Communications Privacy Act).

155. *See EFF Analysis*, *supra* note 123, at 10.

156. *See ACLU Statement*, *supra* note 17 (discussing Operation CHAOS, which involved extensive information sharing between the FBI, CIA, and NSA concerning activities by black nationalists, Vietnam war protesters, and student activists).

157. P.L. 107-56, Title II, § 203(a), 115 Stat. 272 § 203(a) (2001), codified at FED.R.CRIM.P. 6(a). The Act provides in part that "disclosure may be made (to intelligence agencies) when the matters involve foreign intelligence or counterintelligence or foreign intelligence information, to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties." (parenthetical added). *Id.*

158. *Id.* The ACLU takes issue with the sharing of grand jury information with the CIA, pointing out that under the new definition of "foreign intelligence information" would permit information about Americans to be shared with the CIA even if the information was not necessary to national security and even if the information was not limited to the person being investigated. *ACLU Analysis*, *supra* note 28.

CIA with information intercepted from electronic communications.[159] Section 901 of the Act also moves the responsibility for collecting and disseminating intelligence information from the Attorney General to the Director of the CIA.[160]

The Act contains a number of provisions that do not explicitly address terrorism per se but nonetheless have serious Fourth Amendment implications.[161] Various portions of USAPA amend the U.S. Code to allow law enforcement officers acting under color of law to intercept wire transmissions made to or from a particular computer, so long as the officer is lawfully engaged in an investigation, and reasonably believes that the transmissions are relevant to the investigation.[162] Another provision without an overt terrorism-related application provides for the adding of samples to a DNA database for those convicted of violent crimes.[163] Title II further alters The Computer Fraud and Abuse Act, allowing wiretaps to be used in the prosecuting of computer-based crimes.[164]

Section 507 mandates the disclosure of educational records "relevant to. . . an act of domestic or international terrorism."[165] Section 508 amends the (now repealed) National Education Statistics Act of 1994, making it easier for the Attorney General to gain access to educational statistics upon certification from the Attorney General that there are "clear and articulable facts" showing the relevance of

159. P.L. 107-56, Title II, §§ 203(b)(2), 209(1), and 217(1), 115 Stat. 280, 283, 291 (2001), codified as amended at 18 U.S.C. §§ 2510 (2000 & Supp. 2002). *See also* P.L. 107-56, Title II, § 203(b)(1), 115 Stat. 280 (2001), codified as amended at 18 U.S.C. § 2517 (2000 & Supp. 2002) ("Authorization for disclosure and use of intercepted wire, oral, or electronic communications").

160. 50 U.S.C. § 403(c) (2000). The ACLU admits that the language of this section prohibits the CIA Director from conducting electronic surveillance, but does not similarly prohibit physical searches, and argues that the Act has the effect of giving the CIA a significantly enhanced role in the domestic intelligence gathering process, contrary to the provisions of its charter. *See ACLU Commentary*, *supra* note 124 (arguing against the dismantling of inter-agency intelligence-sharing barriers).

161. *See generally EFF Analysis*, *supra* note 124.

162. P.L. 107-56, Title II, §§ 203(b)(2), 209(1), and 217(1), 115 Stat. 280, 283, 291 (2001). This part of USAPA covers activities of "computer trespassers" and also requires that the interception not acquire transmissions other than those to or from the trespasser. *Id.*

163. P.L. 107-56, Title V, § 503, 115 Stat. 364 (2001), codified as amended at 42 U.S.C. § 14135a(d)(2) (2000 & Supp. 2001). Although the section is entitled "DNA identification of terrorists and other violent offenders" it is worth noting that the term "violent offenders" includes a considerable class of persons who are not accused of terroristic offenses. *Id*.

164. P.L. 107-56, Title II, §§ 201, 202, 115 Stat. 278 (2001), codified as amended at 18 U.S.C. § 2516(1)(c) (2000 & Supp. 2003).

165. P.L. 107-56, Title V, § 507, 115 Stat. 367 (2001), codified as amended at 20 U.S.C. § 1232g(j)(A) (2000 & Supp. 2002).

the information to an act of domestic or international terrorism.[166] Some of the most controversial aspects of the bill would permit law enforcement access to public library records.[167] The roving wiretaps permitted by Title II, with their relevant expansions of the information accessible via trap and trace orders, would allow law enforcement officials with a FISC order to access user records for publicly accessible internet terminals and gather lists of email addresses and URLs visited.[168]

One recent lawsuit challenged Section 215 of Title II of the Act.[169] The Plaintiffs in that case, represented by the American Civil Liberties Union, allege that the section unconstitutionally relaxes evidentiary standards, permitting the FBI to obtain warrants without showing probable cause.[170]

In addition to modifying other national security-related functions of law enforcement already discussed, the Act contains many provisions relating to increased emphasis on technological means for ensuring border security.[171] Particularly, the bill authorizes the establishment of a creation of an integrated automated fingerprint system for points of entry.[172] Congress and the President placed provisions in the act urging the implementation of machine-readable passports.[173] Title V ("Removing obstacles to investigating terrorism") presages increased reliance on technological means to manage Federal law enforcement projects.[174] Title VIII

166. *See supra* note 126 and accompanying text (discussing repeal of National Education Statistics Act of 1994). This certification of the Attorney General or Assistant Attorney General does not need to specify what those facts are, and the court does not have the discretion to deny the application. P.L. 107-56, Title V, § 508 (2001).

167. *See The USA PATRIOT Act and Patron Privacy on Library Internet Terminals*, *at* http://www.llrx.com/features/usapatriotact.htm (discussing librarians' fears in the aftermath of September 11, 2001).

168. *See id.* (discussing the expansion of trap and trace orders by analogizing URL information with telephone number information; thus allowing law enforcement officials who have gained a warrant under the reduced FISA standards to view many internet searches conducted by terminal users, as this information appears in the URL window as the search is executed.) *Id.*

169. Muslim Comm. Assoc., discussed *supra* note 14 and accompanying text.

170. Muslim Comm. Assoc. at ¶ 2 of Plaintiff's Complaint for Declaratory and Injunctive Relief. The Complaint notes that under Section 215, parties served with such warrants are prohibited from ever disclosing to the target that the FBI has sought the requested information, records or items. *Id.*

171. *See generally* P.L. 107-56, Title IV (2001) (attempting to address issues such as the unprotected U.S./Canadian border, the longest unprotected border in the world).

172. P. L. 107-56, Title IV, § 405 (2001).

173. *Id.* at § 417 ("Machine readable passports).

174. *See* press release, *Attorney General Ashcroft Directs Law Enforcement*

("Strengthening the criminal laws against terrorism") mandates activity to deter cyberterrorism,[175] and supports the development of new Federal cybersecurity forensic capabilities.[176]

X. CONCLUSION

Certain provisions of USAPA are unconstitutional to the extent that they cast too wide a net over too much constitutionally-protected activity. By relaxing warrant requirements, the Congress evokes memories of dark times, when law enforcement officials spied on Americans based solely on their political associations. Every effort must be made to protect the delicate balance between fundamental liberties and national security, notwithstanding the tremendous fear of terrorism. It remains important for the current judiciary to remain a bulwark against a return to some of our most shamefully repressive periods. The pace of technological advancement must not eclipse the pace of legislative and judicial and executive evolution.

Portions of USAPA are reasonable inasmuch as they enhance law enforcement's power to communicate and efficiently prosecute suspected terrorists, however "sneak-and-peek" warrants are anathema to the established principle that notice be given to the suspect that a search has been conducted. It is also unconstitutionally overbroad to define terrorism in such a way as to encompass so much legal and benign political activity. It is likewise unconstitutional and un-American to apply warrants so vague they place no constraints upon the prosecution, that require no offense to be specified, no particular party or evidence to be targeted. Such provisions of the Act ought to be construed severely by the courts. If an officer of the law may obtain a warrant upon speculation as to relevancy to a criminal investigation, then both he and the court violate the Fourth

Officials to Implement New Anti-Terrorism Act, at http://www.usdoj.gov/opa/pr/2001/01_ag_558.htm (on file with author). The press release announces "Investigators will now aggressively pursue terrorists on the internet," and quotes the Attorney General, who claims that "law enforcement is now empowered with new tools and resources necessary to disrupt, weaken, and eliminate the infrastructure of terrorist organizations. . ." *Id.*

175. P.L. 107-56, Title VIII, § 814 (2001) ("Deterrence and Prevention of Cyberterrorism"). Cyberterrorist strikes take forms similar to that of the attack occurring on October 23, 2002 which affected 9 of the 13 root-level internet servers. Alberti, Bob, *Perspective: Waiting for the Net Meltdown, at* http://news.com.com/2010-1071-9632905.html (on file with author). An attack successfully targeting all 13 would have the effect of severely affecting global internet use. *Id.* Although this attack was not discernable to almost any user, some news sources estimate that overall internet responsiveness and access was reduced by six percent. *Id.*

176. P.L. 107-56, Title VIII, § 816 (2001).

Amendment. Courts should invalidate provisions of USAPA permitting "roving wiretaps," but it is unlikely that they will do so in the short term. Yet, the great strength of the Constitution is its flexibility, and it will endure. The pendulum swings both ways, and now it is upon us to guard our liberties more closely so that they will remain. And so we shall.