NOTE

THE ROLES OF THE JUDICIARY IN EXAMINING AND SUPERVISING THE CHANGING LAWS OF ELECTRONIC SURVEILLANCE

*Jie Xiu**

TABLE OF CONTENTS

* B.A., English Information Management, Beijing Foreign Studies University; M.A., English Translation, University of International Business and Economics; J.D., Seton Hall University School of Law, anticipated 2004.

I. Introduction

Following the terrorist attacks of September 11, 2001, Congress moved with tremendous alacrity to authorize new powers for the federal government in an effort to prevent future terrorism. Less than six weeks after the terrorist attacks, Congress endorsed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("the USA PATRIOT Act"),[1] which was signed into law by President George W. Bush on October 26, 2001.[2] The Act grants additional wiretapping and surveillance authority to federal law enforcement and removes barriers between law enforcement and intelligence agencies.[3]

The surveillance power expansion sought by the government has given rise to legal challenges of constitutional dimensions. Indeed, many courts are now faced with the judicial task of balancing the concerns and fears of national security against the people's constitutional rights in a manner that upholds the spirit of the First and Fourth Amendments of the U.S. Constitution.

This Note will explore the new roles that the judiciary should play in the regulation and supervision of the changing laws of electronic surveillance, with particular concentration on the USA PATRIOT Act[4] and the new Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations (the "Guidelines").[5] It argues that before Congress can immediately incorporate any improvements into the statutory law, courts should assume a more active role in checking the Executive Branch and therefore, make it possible to both protect national security and provide greater protection for privacy than currently exists.

Part I of this Note examines the courts' traditional role and approach adopted for constitutional challenges against electronic surveillance laws.[6] Part II provides an in-depth overview of the current legislation and regulation, which seek to expand government power in

---

1 USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

2 Alison A. Bradley, *Extremism in the Defense of Liberty?: The Foreign Intelligence Surveillance Act and the Significance of the USA Patriot Act*, 77 TUL. L. REV. 465, 467 (2002).

3 *See infra* Part II.A.

4 *See infra* Part II.A.

5 *See infra* Part II.B.

6 *See infra* Part I.

the field of electronic surveillance.[7] Part III examines the courts' recent decisions in response to the changes sought by the government, which reveal the judiciary's struggle in attempting to maintain a fine balance between effective law enforcement and the people's privacy and other constitutional rights.[8] Part IV proposes roles the judiciary should play in the future supervision and enforcement of electronic surveillance law.[9]

II. The Traditional Role of the Judiciary in the Development of Electronic Surveillance Laws

A. *The Evolving Judicial Role*

In the field of electronic surveillance, the role of the judiciary is essential in that it ensures a proper separation of powers and protects individuals from "unreasonable searches and seizures" from the government as provided by the Fourth Amendment.[10] However, the judiciary did not recognize this role at the very beginning of the development of electronic surveillance, although it did recognize that the Fourth Amendment protects personal privacy from physical surveillance.[11]

The courts insisted that the Fourth Amendment protected only physical property interests[12] and refused to expand the Fourth

---

7 *See infra* Part II.

8 *See infra* Part III.

9 *See infra* Part IV.

10 U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . .").

11 In 1877, Fourth Amendment warrant requirements were held applicable to a sealed letter entrusted to the mail. *Ex parte* Jackson, 96 U.S. 727, 733 (1877). The court held that "the constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers thus closed against inspection, wherever they may be." *Id.* In 1881, tort relief was granted in *De May v. Roberts*, 9 N.W. 146 (Mich. 1881), when the court determined that observing childbirth without consent was a violation of privacy. *Id.* at 149. The court opined that the "plaintiff had a legal right to the privacy of her apartment at such a time, and the law secures to her this right by requiring others to observe it, and to abstain from its violation." *Id.*

12 An example of this property-based application is *Boyd v. United States*, 116 U.S. 616 (1886), in which the Court found that compelled production of a person's private papers constituted an unreasonable search and seizure within the meaning of the Fourth Amendment. *Id.* at 634-35. To reach this conclusion, the Court heavily relied upon the English case of *Entick v. Carrington*, 95 Eng. Rep. 807 (K.B. 1765), in 19 Howell's State Trials 1029, finding Lord Camden's pronouncement of the judgment to be "sufficiently

Amendment protections into the area of electronic surveillance. In *Olmstead v. United States*,[13] the Supreme Court ruled that Fourth Amendment protection did not extend to telephone conversations because of the lack of entry, search, and seizure involved in intercepting the conversations.[14] Chief Justice Taft reasoned that when authorities tapped the defendant's phone from outside his home and office, such action did not constitute an "actual physical invasion" or the taking of "tangible material effects."[15]

In his famous dissent, Justice Brandeis vehemently contended that such an interception of communications, even without a physical trespass or seizure of tangible property, constituted an illegal search and seizure under the Fourth Amendment.[16] Most forceful was his argument that the Fourth Amendment embraced a "right to be let alone," and to protect that right, Justice Brandeis asserted that "[e]very unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth."[17]

Although Justice Brandeis's dissent signaled a shift in attitude away from the property-based applications of the Fourth Amendment, the dissent was not seriously considered for almost forty years until the United States Supreme Court again had to address an electronic

---

explanatory of what was meant by unreasonable searches and seizures." *Boyd*, 116 U.S. at 627. In *Entick*, the English court stated that:

> Papers are the owner's goods and chattels; they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and *though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect.*

95 Eng. Rep. 807 (K.B. 1765), in 19 Howell's State Trials 1029; *see also Boyd*, 116 U.S. at 627-28 (emphasis added). The *Boyd* Court reasoned that "[i]t is not the breaking of [a man's] doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property . . . which underlies and constitutes the essence of Lord Camden's judgment." *Boyd*, 116 U.S. at 630.

[13] Olmstead v. United States, 277 U.S. 438 (1928).

[14] *Id.* at 464-65 (rejecting the argument that communications over wires are analogous to mailed letters, which receive Fourth Amendment protection).

[15] *Id.* at 466.

[16] *Id.* at 471-73 (Brandeis, J., dissenting).

[17] *Id.* at 478-79.

surveillance controversy in *Katz v. United States*.[18] In *Katz*, FBI agents—acting without a warrant—set up a wiretap by attaching a listening device to the outside of a public telephone booth from which the appellant was engaging in illegal bookmaking activities.[19] Influenced by notions of privacy, the Court held that "[t]he Government's activities in electronically listening to and recording the petitioners' words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[20] Justice Harlan's concurrence in *Katz* created a two-part test[21] to determine when the Fourth Amendment, which the Court declared "protects people, not places,"[22] actually confers such protection. Responding to the majority holding of *Katz*, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"),[23] as a means to implement a uniform procedure for conducting constitutionally acceptable electronic surveillance.[24]

Although in *Katz*, the Court held that the Fourth Amendment's warrant provision applied to electronic surveillance, it explicitly declined to extend its holding to cases "involving the national security."[25] It was not until 1972, in the decision of *United States v. United States District Court* ("*Keith*"),[26] that the Court first addressed the issue of electronic surveillance in the national security setting.[27]

In *Keith*, the Attorney General authorized warrantless electronic surveillance of the defendant, a United States citizen, suspected of conspiring to destroy government property.[28] Although Justice Powell conceded that the Constitution and Title III may constitute "an implicit

---

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

19 *Id.* at 348.

20 *Id.* at 353.

21 *Id.* at 361. The test requires "first that a person have exhibited an actual (subjective) expectation of privacy, and, second, that the expectation be one that society is prepared to recognize as 'reasonable'." *Id.* (Harlan, J., concurring).

22 *Id.* at 351.

23 Title III, Pub. L. No. 90-351, §802, 82 Stat. 197, 212.

24 *See infra* Part I.B.1.

25 *Katz*, 389 U.S. at 358 n.23 ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.").

26 United States v. United States District Court ("Keith"), 407 U.S. 297 (1972).

27 *Id.* at 299.

28 *Id.*

recognition"[29] of the President's constitutional authority to protect the nation's security, the Justice concluded the "language is essentially neutral" concerning the President's electronic surveillance power, and that it does not confer upon the President additional power to unilaterally order or permit electronic surveillance.[30]

Justice Powell reasoned that waiving the Fourth Amendment probable cause requirement could lead the executive to easily forego people's privacy and free speech rights.[31] Justice Powell concluded that maintaining separation of powers among the different branches and levels of government and protecting individual freedoms requires a judicial role in issuing warrants.[32]

The government argued for an exception to the warrant requirement, citing the unique features of ongoing national security intelligence gathering, the complexity of factors involved, and the danger of leaks.[33] The Court, however, determined that the potential for abuse of the surveillance power in this context, along with the Court's competence in dealing with highly complex matters and the Court's ability to protect sensitive information in an *ex parte* proceeding, justified a denial of the exception.[34] Justice Powell wrote that the inconvenience to the government is "justified in a free society to protect constitutional values."[35]

While the majority in *Keith* held that the President has no power to unilaterally order or permit electronic surveillance in the national security setting, it emphasized that this case involved only the domestic aspects of national security.[36] Finally, the Court left open the possibility that different warrant standards and procedures than those required in a normal criminal investigation might be applicable in a national security investigation.[37]

---

29 *Id.* at 303.

30 *Id.*

31 *Keith*, 407 U.S. at 317.

32 *Id.*

33 *Id.* at 318-19.

34 *See id.* at 319-20.

35 *Id.* at 321.

36 *Id.* at 321-22 ("We . . . express no opinion as to the issues which may be involved with respect to activities of foreign powers or their agents.").

37 *See id.* at 322 (recognizing the national security surveillance can require more time, more sources, more types of information, focus more on prevention or preparedness, and generally lack the precision of ordinary criminal cases).

Although Congress did not react immediately to the *Keith* Court's invitation for a set of standards for such surveillance, it provided an important impetus for the legislation to develop them.[38] In 1978, President Carter signed into law the Foreign Intelligence Surveillance Act of 1978 ("FISA").[39] The Act included a "quasi-criminal" targeting standard and more limited protections for aliens representing foreign governments in the United States.[40]

B. *Title III and FISA*

Title III and FISA are two major laws that have governed the FBI's electronic surveillance.[41] Title III governs warrants in criminal investigations,[42] but FISA applies to national security investigations.[43]

1. Title III

Title III was the legislative response to the United States Supreme Court's landmark decision in *Katz*.[44] Pursuant to Title III, law enforcement agencies must obtain warrants before engaging in surveillance activities for criminal investigative purposes.[45] To grant such a warrant, the judge must find probable cause that a serious crime has been or is about to be committed.[46] The probable cause requirement is a substantial threshold that the surveillance applicant must reach before obtaining the wiretap authority. It protects against unreasonable searches and seizures as provided by the Fourth Amendment.

Generally, all criminal surveillance must be authorized by a judge

---

38 Sharon H. Rackow, *How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of 'Intelligence' Investigations*, 150 U. PA. L. REV. 1651, 1661-62 (2002).

39 The Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§1801-11 (1994 & Supp. IV 1998)), *amended by* Act of Dec. 3, 1999, Pub. L. No. 106-120, 113 Stat. 1606.

40 *See* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 811 (1989).

41 *See* Rackow, *supra* note 38, at 1657-58.

42 *See infra* Part I.B.1.

43 *See infra* Part I.B.2.

44 *See supra* pp. 5-6.

45 18 U.S.C. § 2518 (3)(a) (1994).

46 18 U.S.C. § 2516 (1) (1994). Section 2516 (1) enumerates crimes that an interception must be able to disclose before a judge can authorize the interception. *Id.*

of competent jurisdiction.[47] In an emergency situation,[48] however, law enforcement may engage in warrantless wiretapping, so long as an application for a warrant is made within forty-eight hours of the commencement of interception.[49]

Although Title III is broad in scope, it is clear that the statute was not meant to infringe upon the Executive's long-standing surveillance authority over matters concerning foreign intelligence.[50]

2. FISA

In the early 1970s, the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the "Church Committee") conducted an investigation of the United States intelligence agencies to determine the extent of alleged invasions of individual privacy interests.[51] The Church Committee Report revealed widespread warrantless electronic surveillance of individuals who were not associated in any way with a foreign power, did not seem to pose a threat to national security, and were not suspected of being involved in criminal activities.[52] These findings compelled Congress to pass FISA in 1978, which definitively determines the role of the Executive in authorizing intelligence surveillance of foreign powers and individuals engaged in activities deemed to threaten national security.[53]

FISA provides statutory authorization for electronic surveillance in the limited context when surveillance is sought to target a foreign power or an agent of a foreign power,[54] and when the purpose of the

---

47 18 U.S.C. § 2518 (1) (1994); *see also* 18 U.S.C. § 2516 (1994).

48 18 U.S.C. § 2518 (7)(a)(iii) (1994). An emergency situation is where there is immediate danger of death or serious injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime. *Id.*

49 18 U.S.C. § 2518 (7) (1994).

50 18 U.S.C. § 2511(2)(e)(f) (1994) ("'[N]othing contained in this chapter . . . shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications.").

51 *See* Cinquegrana, *supra* note 40, at 806-07.

52 *Id.* at 806-07.

53 *Id.* at 807.

54 50 U.S.C. § 1804 (a)(4)(A) (1994). FISA broadly defines the term "foreign power" as a foreign government, a faction of a foreign nation, a group engaged in international terrorism, an entity directed and controlled by a foreign government, or a foreign-based political organization not substantially composed of United States Persons. 50 U.S.C. § 1801(a) (1994). An "agent of a foreign power" is defined as any non-United States person who: acts in the United States as an officer, employee, or member of a foreign power; or

surveillance is to obtain foreign intelligence information.[55] Each application for surveillance authorization must be made by a federal officer, with the approval of the Attorney General, to the Foreign Intelligence Surveillance Court ("FISC").[56] FISA mandates the formation of this special court, which consists of seven district court judges appointed by the Chief Justice of the United States, to hear all FISA applications for electronic surveillance.[57]

A FISC judge is permitted to authorize a FISA surveillance if the judge finds, among other factors,[58] that

> [T]here is probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment.[59]

Each federal officer seeking surveillance authority must satisfy the numerous application criteria explicitly laid out in § 1804 of FISA.[60] Although these extensive requirements suggest that the applying federal officer must have engaged in a thorough investigation of the target to supply the court sufficient information, none of the criteria rise to the level of the Fourth Amendment's probable cause requirement. The

---

acts on behalf of a foreign power engaging in clandestine intelligence activities in the United States. 50 U.S.C. § 1801(b)(1) (1994).

55 50 U.S.C. § 1804 (a)(7)(B) (1994).

56 50 U.S.C. § 1804 (a) (1994).

57 50 U.S.C. § 1803 (1994).

58 50 U.S.C. § 1805 (a)(1)-(5) (1994). The other factors include that the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information, that the application has been made by a Federal officer and approved by the Attorney General, that there is probable cause to believe that each site of surveillance is being used, or is about to be used, by a foreign power or an agent of a foreign power, that the proposed minimization procedures meet the statutory requirement, and that the application which has been filed contains all statements and certifications specified by the statute. *Id.*

59 50 U.S.C. § 1805 (a)(3)(A) (1994).

60 50 U.S.C. § 1804 (1994). The application criteria include but are not limited to: the identity or a description of the target, the facts or circumstances leading the applicant to believe that the target is a foreign power or an agent of a foreign power, that each of the sites of surveillance is being used or is about to be used by a foreign power or an agent of a foreign power, a statement of the proposed minimization procedures, a detailed description of the nature of the information sought, that a certifying official deems that the information sought is foreign intelligence information, that such information cannot reasonably be obtained by normal investigative techniques, and that the purpose of the surveillance is to obtain foreign intelligence information. *Id.*

federal officer does not need to demonstrate that a criminal or unlawful act has been or is about to be committed before the officer is granted authority to intrude upon the privacy interests of the specified target.[61] Theoretically, the officer is not seeking evidence of criminal activities on which to base a prosecution, but rather is seeking information regarding foreign intelligence activities that may compromise national security.

Once the Attorney General certifies the application of a federal officer, the surveillance request is "subjected to only minimal scrutiny by the courts."[62] According to the Center for Democracy and Technology, the FISA court, which approved more than 1,000 surveillance requests last year, has denied only one request in 22 years.[63]

II. Changing Laws

A. *The USA PATRIOT Act*

The USA PATRIOT Act[64] was signed into law by President Bush on October 26, 2001. The Act authorizes broad expansion of the government's power to engage in electronic surveillance.

The Act first allows the government to monitor the private telephone conversations of individuals suspected of purely domestic criminal activity under the guise of an 'intelligence' investigation, without demonstrating probable cause that a crime has been or is soon to be committed.[65] Now, in an application to the FISC, a federal officer no longer has to demonstrate that "the purpose of the surveillance is to obtain foreign intelligence information,"[66] but may obtain surveillance authorization under the less stringent showing that "a significant purpose of the surveillance is to obtain foreign intelligence information."[67] Thus, it is extremely likely that the amended FISA will

---

61 50 U.S.C. § 1801 (b)(2)(A) (1994). If a given target is a United States person, the most a federal officer will need to demonstrate to the FISC is that the target's activities "involve or may involve a violation of the criminal statutes of the United States"— a low threshold of proof to obtain surveillance authorization. *Id.*

62 United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984).

63 Marcia Coyle, *Sharp Debate on Surveillance Law: Pick Between Two Little Words Makes a Big Difference*, NAT'L L.J., Oct. 8, 2001, at A13.

64 *See supra* note 1.

65 USA PATRIOT Act § 218 (2001) (amending §1804 (a)(7)(B) of FISA).

66 50 U.S.C. § 1804 (a)(7)(B) (1994).

67 USA PATRIOT Act § 218 (2001).

be used as a means to undertake surveillance without demonstrating the heightened standard of probable cause required under Title III for criminal wiretaps.[68]

Second, the Act allows the government to overhear private conversations of non-suspects by extending roving wiretap authority to foreign intelligence investigations without proper privacy protections. In 1986, Congress amended Title III to allow for "roving wiretaps" in criminal investigations.[69] A Title III roving wiretap allows law enforcement agents to intercept only those conversations when the agents reasonably believe the target is using a particular phone.[70] The USA PATRIOT Act extends Title III's roving wiretap authority to FISA.[71] Yet, it does not contain the "reasonably proximate" privacy protection provision of Title III. Therefore, an agent may now wiretap a telephone in an innocent individual's home for the entire day regardless of whether the target is actually using the phone or has already left the location.[72]

Third, the government can intercept communications from the Internet, including electronic mail and Web surfing, which far exceed the definition of pen register and trap and trace devices under FISA.[73] Previously under FISA, a pen register or trap and trace order only

---

[68] *See* 147 CONG. REC. S10,593 (daily ed. Oct. 12, 2001) (statement of Sen. Leahy). Senator Leahy recognized that by amending the language of FISA, "the USA Act would make it easier for the FBI to use a FISA wiretap to obtain information where the Government's most important motivation for the wiretap is for use in a criminal prosecution." *Id.* He further acknowledged that "[t]his is a disturbing and dangerous change in the law." *Id.*

[69] 18 U.S.C. § 2518 (11) (1994). If law enforcement agents could demonstrate to the reviewing judge that a suspect purposely was changing telephones as a means to thwart previously authorized governmental wiretaps, they could obtain a "roving" wiretap warrant—allowing agents the ability to target their surveillance on an individual, rather than a particular telephone. *Id.*

[70] 18 U.S.C. § 2518 (11)(b)(iv) (1994) (law enforcement should determine whether the target actually was using the phone line or was reasonably proximate to the instrument through which such communication will be or was transmitted).

[71] USA PATRIOT Act § 206 (2001) (amending § 105(c)(2)(B) of FISA).

[72] *See* Rackow, *supra* note 38, at 1681.

[73] According to the original Pen/Trap statute (Chapter 205 of Title 18 of the US Code), a "pen register" device was a device that "records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted" on the telephone line to which it is attached. 18 U.S.C. § 3127 (3) (1994). A "trap and trace" device was a device that "captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." 18 U.S.C. § 3127 (4) (1994).

required a telephone company to reveal the numbers dialed to and from a particular telephone.[74] The standard of proof required for this type of warrant is very low and only requires activity "relevant to an ongoing criminal investigation."[75] The USA PATRIOT Act expands the definition of pen register and trap and trace devices to encompass communications from the Internet, including electronic mail and Web surfing.[76] The problem, however, is that these types of communication contain data that is far more revealing than telephone numbers.[77] Therefore, probable cause, usually required for obtaining content, is ignored.

Fourth, the Act discourages political dissent by including the activities of unpopular political organizations within the newly created definition of "domestic terrorism."[78] Under this expansive definition, many acts of political dissent and activism, such as those of anti-abortion activists who use violence against women entering Planned Parenthood clinics, World Trade Organization protestors who threw rocks through the windows of merchants and politicians who publicly supported the WTO, now will be characterized as "domestic terrorism."[79] The government may use this new definition as a means to

---

[74] 18 U.S.C. § 3122 (b)(2) (1994).

[75] *See* ACLU, *How the USA PATRIOT Act Limits Judicial Oversight of Telephone and Internet Surveillance*, *at* http://www.ACLU.org/congress/l102301g.html (last modified Oct. 23, 2001), note 154.

[76] USA PATROT Act § 216(a) (2001). A "pen register" is a "device or process" that "records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." *Id.* A "trap and trace" device is a "device or process" that "captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signalling information reasonably likely to identify the source of a wire or electronic communication." *Id.*

[77] Jennifer C. Evans, *Hijacking Civil Liberties: The USA PATRIOT Act of 2001*, 33 LOY. U. CHI. L.J. 933, 977 (2002).

[78] USA PATRIOT Act § 802 amends 18 U.S.C. § 2331, which defines international terrorism, by instituting a new crime of "domestic terrorism." USA PATRIOT Act § 802 (2001). It broadly defines "domestic terrorism" as activities that –involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, § 802(5)(A); appear to be intended –(i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping, § 802(5)(B); and occur primarily within the territorial jurisdiction of the United States, § 802(5)(C). *Id.*

[79] *See* 147 CONG. REC. H6,768 (daily ed. Oct. 12, 2001) (statement of Rep. Paul). Representative Paul cautioned:

> Under this broad definition, should a scuffle occur at an otherwise peaceful pro-life demonstration the sponsoring organization may become the target of a

silence or prosecute political protestors and dissidents.

Finally, the Act expands the sharing of sensitive information between intelligence agencies and law enforcement. The Act allows law enforcement officers to share electronic, wire and oral interception information with any other law enforcement officers and intelligence agencies to the extent that such contents include foreign intelligence or counterintelligence.[80] The effect is to allow sharing of wiretap information with any federal agency, including the CIA and INS, whereas previously such sharing had to be related to the same investigation that initially gave rise to the wiretap.[81] This new provision is an important component of the Justice Department's desire to build a general federal database of all criminal information.[82]

B. *Attorney General's Guidelines*

On May 30, 2002, the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations (the "Guidelines") were released. The Guidelines, in existence since 1976, provide general guidance for the FBI's investigations of crime and criminal intelligence by classifying various types of crimes and their investigations and delineating the methods and scope of such investigations.[83] According to Attorney General John

---

> federal investigation for terrorism. We have seen abuses of law enforcement authority in the past to harass individuals or organizations with unpopular political views. I hope my colleagues consider that they may be handing a future administration tools to investigate pro-life or gun rights organizations on the grounds that fringe members of their movements advocate violence. It is an unfortunate reality that almost every political movement today, from gun rights to environmentalism, has a violent fringe.

Id.

[80] USA PATRIOT Act § 203 (b) (2001) (amending 18 U.S.C. §2517).

[81] *See* USA PATRIOT Act § 203 (d) (2001) (authorizing foreign intelligence or counterintelligence to be disclosed to any federal law enforcement official to aid the official receiving that information in the performance of his official duties).

[82] *See* USA PATRIOT Act § 105 (2001) (explaining that the Director of the United States Secret Service shall take appropriate actions to develop a national network of electronic rime task forces).

[83] *See* David M. Park, *Re-Examining the Attorney General's Guidelines for FBI Investigations of Domestic Groups*, 39 ARIZ. L. REV. 769 (1997). Shortly after the revelation of the Church Committee's Report, *supra* Part I.B.2, then Attorney General Edward Levi was compelled to develop a written set of guidelines to govern FBI investigations. *Id.* at 772. The Levi guidelines focused on freedom of speech and freedom of the press. *Id.* Investigations based solely on unpopular speech, where there is no threat of violence, were prohibited. *Id.* In 1983, Attorney General William French Smith

Ashcroft, the reissued Guidelines are intended to encapsulate four "overriding principles": first, that "the war against terrorism is the central mission and highest priority of the FBI;" second, that the prevention of terrorism is "the key objective;" third, that the effective detection, investigation and prevention of terrorism should not be hindered by unnecessary red tape and bureaucracy; and fourth, that in identifying potential terrorist threats, the FBI must "draw proactively on all lawful sources of information."[84]

Under these principles, FBI agents could enter and observe public places and forums as any member of the public might.[85] They are also empowered to scour public sources for information on future terrorist threats even absent specific investigative predicate.[86]

The lack of judicial oversight, and the generality and breadth of the Guidelines, have raised the ire of privacy advocates, who believe that the Guidelines allow the FBI to go on "fishing expeditions" where there

---

developed a new set of regulations, which superseded Levi's original Guidelines regarding domestic investigations. *Id.* The new rule was entitled The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations. *Id.* The Smith Guidelines were intended to increase the investigative avenues available to the FBI in domestic terrorism cases. *Id.* It altered the Levi standard requiring the FBI to base their security investigations on "specific and articulable facts." *Id.* The investigation may be initiated "when the facts or circumstances reasonably indicate that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals... through activities that involve force or violence and a violation of the criminal laws of the United States." *The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations*, 32 CRIM. L. REP. (BNA) 3087, 3091-92 (Mar. 2, 1983). The "reasonable indication" standard is significantly lower than the Fourth Amendment standard of probable cause required in law enforcement. Park, at 722. The Smith Guidelines also allowed for more invasive techniques. *Id.* The only techniques it specifically bar were mail covers, mail openings, and nonconsensual electronic surveillance. *Id.* It stressed that agents used the least intrusive means available. Attorney General John Ashcroft's Guidelines is the third in the line and supersedes all the previous ones.

[84] *Remarks of Attorney General John Ashcroft— Attorney General Guidelines, May 30, 2002, available at* http://www.fas.org/irp/news/2002/05/ag053002.html (last accessed Jan. 4, 2003). The text of the Guidelines are available from the website of the US Department of Justice's Office of Legal Policy, *at* http://www.usdoj.gov/olp/generalcrimes2.pdf (last accessed Jan. 4, 2003).

[85] *See id.*

[86] *See id.*; *see also the Guidelines, Part VI*, which authorizes such activities as "surfing the Internet as any member of the public might do . . . to detect terrorist and other criminal activities," and tracking foreign terrorists by combining its investigative results with information obtained from other lawful sources, such as foreign intelligence and commercial data services. *Id.*

is no evidence that a crime has been or will be committed.[87]

III. The Judiciary's Reactions

With increasing speed, the Justice Department of Attorney General John Ashcroft is starting to make an open book of the lives of hundreds of thousands of Americans. The surveillance campaign is being carried out by every major FBI office in the country, which involves twenty-four-hour monitoring of the suspects' telephone calls, e-mail messages and Internet use, as well as scrutiny of their credit card charges, their travel and their visits to neighborhood gathering places, including mosques.[88]

Even the FBI officials concede that the domestic threat posed by al Qaeda cells may at times have been overstated, especially after the arrest on May 8, 2002 of Jose Padilla, an American also known as Abdullah al-Muhajir.[89] Justice Department officials have abandoned their initial suggestion that they had compelling evidence linking him to a plot to build an explosive radiological device known as a dirty bomb.[90] As people are getting more and more concerned about law enforcement's expanded investigative powers, the judiciary is struggling to maintain a fine line between effective law enforcement and the protection of individual privacy.[91]

---

[87] *See* the American Civil Liberties Union's ("ACLU") open letter, *Analysis of Legal Changes to the Attorney General Guidelines, 5 June 2002, available at* http://www.aclu.org/Congress/1060602c.html (last visited Oct. 12, 2002).

[88] Philip Shenon & David Johnston, *Seeking Terrorist Plots, F.B.I. Is Tracking Hundreds of Muslims, at* http://www.nytimes.com/2001/10/06/national/06SLEE.html/todaysheadlines (last visited Oct. 17, 2002).

[89] *See id.* Abdullah al Muhajir, 31, is a former street gang member born in Brooklyn as Jose Padilla. He had been under surveillance overseas by the CIA and FBI, and was arrested on May 8, 2002 at O'Hare International Airport in Chicago after arriving on a flight from Pakistan. Dan Eggen & Susan Schmidt, *"Dirty Bomb" Plot Uncovered, U.S. Says: Suspected Al Qaeda Operative Held As "Enemy Combatant,"* WASH. POST, June 11, 2002, at A1. U.S. officials said that he had close connections with al Qaeda, and that he was scouting targets after learning how to build a dirty bomb in Pakistan and Afghanistan. *Id.* Bush administration officials characterized the case as "the most specific plot disrupted by the U.S. government since September 11," though they admitted that there was not an actual plan yet. *Id.*

[90] *See* Shenon & David, *supra* note 88.

[91] *See infra* Part III.A-C.

A. *The Open Opinions by the FISA Courts*

The two open opinions issued by the "super-secret" FISA court and its review court reflect a contradicting view among the judiciary regarding how courts should proceed under changing electronic surveillance law.

The FISC opinion was issued on May 17, 2002.[92] The FISA court rarely issues an open opinion and the May 17 ruling was only the second in its quarter-century history.[93] All seven judges of the court unanimously criticized federal agents for misleading the court in applications for secret eavesdropping warrants on seventy-five occasions during the Clinton Administration (as of September 2000) and an unspecified additional number between September 2000 and March 2001.[94]

The court found that the Justice Department wanted to use the USA PATRIOT Act improperly when it moved for the court to approve proposed minimization procedures,[95] entitled "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI," for use in electronic surveillances and physical searches authorized by the court.[96]

In order to make sure that FISA surveillances and searches were not being used *sub rosa* for criminal investigations, the court routinely approved the use of information screening "walls" proposed by the government in its applications.[97] However, the court found that the

---

[92] *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (May 17, 2002).

[93] *See* James Bamford, *Washington Bends the Rules*, *at* http://www.nytimes.com/2002/08/27/opinion/27BAMF.html (Aug. 27, 2002).

[94] *See In Re* All Matters, 218 F. Supp.2d at 620.

[95] The FISA Act, §§ 1801(h)(1), 1821(4)(A) (1994). Minimization procedures are "specific procedures, which shall be adopted by the Attorney General, in surveillance, search to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of foreign intelligence information gathering." *Id.*

[96] *See In Re* All Matters, 218 F. Supp.2d at 615.

[97] *See id.* at 620. Under the normal "wall" procedures, a screening mechanism, or person, usually the chief legal counsel in a FBI field office, or an assistant U.S. attorney not involved in the overlapping criminal investigation, would review all of the raw intercepts and pass on only relevant information. *Id.* In "significant cases, involving major complex investigations such as the bombings of the U.S. Embassies in Africa, and the millennium investigations," when criminal investigations and prosecutions were likely, the court became the "wall" so that FISA information could not be disseminated to criminal prosecutors without the court's approval." *Id.*

"wall" between intelligence and criminal investigations was breached in an "alarming number of instances."[98] The proposed minimization procedures even further amplified a criminal prosecutor's role in directing FISA surveillances and searches and guiding them to criminal prosecutions.[99] The government makes no secret of this policy, asserting that the "USA Patriot Act allows FISA to be used for 'a significant purpose,' rather than the primary purpose, of obtaining foreign intelligence information," so as to allow "FISA to be used primarily for a law enforcement purpose, as long as a significant foreign intelligence purpose remains."[100]

Unanimously disagreeing with the Attorney General's position, the court ruled that "the proposed procedures are not consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information, and therefore must be modified."[101]

The May 12 opinion is a bold and significant step by the judiciary to restrain the government's practices of investigating domestic criminal activities under the guise of an intelligence investigation, and sharing sensitive information between intelligence agencies and law enforcement. However, this victory for civil libertarians did not last long since the decision was overturned by the United States Foreign Intelligence Surveillance Court of Review on November 18, 2002.[102]

The United States Foreign Intelligence Surveillance Court of Review has "the distinction of being the only court in the United States

---

98 *Id.* In "September 2000, the government came forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States." *Id.* In virtually every instance, the government's misstatements and omissions in FISA applications involved information sharing and unauthorized disseminations to criminal investigators and prosecutors. *Id.* In "March of 2001, the government reported similar misstatements in another series of FISA applications in which there was supposedly a 'wall' between separate intelligence and criminal squads in FBI field offices to screen FISA intercepts, when in fact all of the FBI agents were on the same squad and all of the screening was done by the one supervisor overseeing both investigations." *Id.*

99 *See id.* at 623. The court found that the provisions that authorize criminal prosecutors to advise FBI intelligence officials on the initiation, operation, continuation or expansion of FISA's intrusive seizures, are designed to "enhance the acquisition, retention and dissemination of evidence for law enforcement purposes, instead of being consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information as mandated in § 1801(h) and § 1821(4)." *Id.*

100 *Id.* Ashcroft *citing* 50 U.S.C. §§1804(a)(7)(B), 1823(a)(7)(B).

101 *Id.* at 625.

102 *See In re*: Sealed Case Nos. 02-001, 02-002, 310 F.3d 717 (Nov. 18, 2002).

that has never heard a case."[103] The court met on September 9, 2002, for the first time in its twenty-four-year history, to consider the government's appeal.[104] The three-judge panel found that "the restrictions imposed by the FISA court are not required by FISA or the Constitution,"[105] and that the Justice Department's proposed use of the USA PATRIOT Act "is constitutional because the surveillances it authorizes are reasonable."[106]

The court of review noted that several federal courts had held that surveillance under FISA was appropriate only if foreign intelligence surveillance was the government's primary purpose.[107] If the primary purpose was not foreign intelligence gathering, but gathering evidence for criminal prosecution, the target was entitled to the traditional protections of the Fourth Amendment, such as a warrant supported by probable course.[108]

---

[103] James Bamford, *Washington Bends the Rules*, *available at* http://www.nytimes.com/2002/08/27/opinion/27BAMF.html?ex=1021481419&ei=1&en=438da4cf0764e7d1 (Aug. 27, 2002).

[104] Philip Shenon, *Secret Court Weighs Wiretaps*, N.Y. TIMES, Sept. 10, 2002, at A12.

[105] *See In re*: Sealed Case Nos. 02-001, 02-002, 310 F.3d at 720. The FISA court imposed certain restrictions on the FBI's surveillance. *Id.* In particular, the court ordered that

> law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division [of the Department of Justice] shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives.

Id.

[106] *Id.* at 746.

[107] *Id.* at 725-26.

[108] *Id.* In *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), the court held that when the object of search or surveillance is a foreign power, its agent or collaborators, the government will be relieved of seeking warrant only when the surveillance is conducted "primarily" for foreign intelligence. *Truong*, 629 F.2d at 915. The court rejected the government's assertion that "if surveillance is to any degree directed at gathering foreign intelligence, the executive may ignore the warrant requirement of the Fourth Amendment." *Id.* Several circuits have followed *Truong*'s "primary purpose" test, despite the fact that *Truong* was not a FISA decision. In *United States v. Megahey*, 553 F.Supp. 1180 (E.D.N.Y. 1982), *aff'd sub nom*, United States v. Duggan, 743 F.2d 59 (2d Cir. 1984), the district court acknowledged that surveillance under FISA would be "appropriate only if foreign intelligence surveillance is the Government's primary purpose." *Megahey*, 553 F.Supp. at 1189-90. On appeal, the Second Circuit endorsed the *Megahey*

Believing that none of these circuit courts could tie the "primary purpose" test to actual statutory language, the special appeals court wrote that "[i]n sum, we think that the FISA as passed by Congress in 1978 clearly did not preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution."[109]

The appeals court also agreed with the government's argument about the constitutionality of amendments to FISA by the USA PATRIOT Act.[110] The court reasoned that:

> [t]he Patriot Act amendment, by using the word 'significant,' eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counter intelligence responses. If the certification of the applicant's purpose articulates a broader objective than criminal prosecution, . . .the government meets the statutory test.[111]

Further, the court reasoned that the FISA procedures come close to meeting Fourth Amendment warrant standards, and that the "surveillances it authorizes are reasonable" as the country is facing the greatest threat to its security.[112]

The order by the Foreign Intelligence Surveillance Court of Review represents a legal triumph for Attorney General Ashcroft, who had pushed for broader powers, and a clear setback for civil libertarians who worried that the new measures would jeopardize the constitutional rights of U.S. citizens. The American Civil Liberties Union ("ACLU") and the National Association of Criminal Defense Lawyers ("NACDL")

---

dichotomy between criminal investigation and foreign intelligence surveillance, and agreed that the surveillance in question was not "directed towards criminal investigation or the institution of a criminal prosecution." *Duggan*, 743 F.2d at 78 (quoting *Megahey*, 553 F.Supp. at 1190). Two other circuits, the Fourth and the Eleventh, have similarly approved district court findings that the surveillance in question was primarily for foreign intelligence purposes. *See* United States v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987), *cert. denied*, 486 U.S. 1010 (1988); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987), *cert. denied,* 485 U.S. 937 (1988). Then, the First Circuit, seeing *Duggan* as following *Truong*, explicitly interpreted FISA to mean that "[a]lthough evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance. " United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991), *cert. denied*, 506 U.S.816 (1992).

109 *In re*: Sealed Case Nos. 02-001, 02-002, 310 F.3d at 727.

110 *Id.* at 735.

111 *Id.*

112 *Id.* at 746.

are exploring a possible appeal to the United States Supreme Court.[113]

B. *The Supreme Court's Recent Decisions on Electronic Privacy Issues*

It is difficult to predict the United States Supreme Court's response to the special appeals court's decision if the ACLU and NACDL succeed in having it appealed. The 2000-2001 term of the Supreme Court produced two excellent examples of the continuing disagreement among the judiciary that swirls around the clash between people's privacy and modern surveillance technologies. In the context of the newly-declared campaign against terrorism, as clashes between competing claims to solitude and security are increasing rapidly, the two Court decisions— *Kyllo v. United States*[114] and *Bartnicki v. Vopper*[115] — deserve special attention in revealing the analytic struggle the Court is undertaking when confronted with such issues.

The collisions in the two cases took place in different contexts. *Kyllo* involved a privacy-based challenge to the search of a home by government agents using a heat detection device.[116] *Bartnicki*, on the other hand, involved a privacy-based challenge to the broadcast of an illegally intercepted cell phone call.[117] Two common threads bring them together: both challenges are based on claims to privacy, and the invasion of privacy is, in turn, based on new technologies. Nevertheless, the United States Supreme Court has reached different conclusions when comparing the privacy right with other recognized rights and policies.

In *Kyllo*, the Court had to decide the issue of whether the use of a thermal imaging device to scan the suspect's house constituted a "search" within the scope of the Fourth Amendment, and hence, would have been presumptively unreasonable if performed without the requisite warrant.[118] The government investigators had used a thermal imager[119] to detect unusually high amounts of heat emanating from a

---

[113] Dan Eggen, *Justice Department Wins Wiretap Ruling*, *available at* http://news.findlaw.com/wp/docs/terrorism/fisa111802opn.pdf (Nov. 18, 2002).

[114] Kyllo v. United States, 533 U.S. 27 (2001).

[115] Bartnicki v. Vopper, 532 U.S. 514 (2001).

[116] *Kyllo*, 533 U.S. at 29.

[117] *Bartnicki*, 532 U.S. at 517.

[118] *Kyllo*, 533 U.S. at 29.

[119] *Id.* at 29-30. Thermal imagers detect infrared radiation and convert it into images

suspect's home.[120] Based upon that discovery, investigators obtained a search warrant[121] and found marijuana plants being grown in the suspect's home.[122] The Court ruled that surveillance of this type—where an instrument "not in general public use" was employed "to explore details of the home that would be previously unknowable without physical intrusion"— was different from purely "visual surveillance" (i.e., "naked eye" surveillance).[123] The Fourth Amendment draws a firm and bright line at the entrance to a person's home and all details occurring within that home are "intimate details" that should be "safe from prying government eyes."[124]

In *Bartnicki*, the Court dealt with a fairly unusual situation where a telephone call, involving a union official who was engaged in aggressive contract negotiations with a school board, was intercepted by an unknown person, who then sent the recording to an official of another organization in opposition to the union.[125] That official in turn provided the recording to a local radio station who then broadcasted it.[126] The Court ruled that the broadcast of an illegally intercepted telephone call still constitutes free speech that is protected by the First Amendment.[127] In refuting the government's argument that the alleged violation of the federal wiretap law[128] breached people's privacy of communication, the Court emphasized that "privacy concerns give way when balanced against the interest in publishing matters of public importance. . . .One of the costs associated with participation in public affairs is an attendant loss of privacy."[129] Because the radio station was "not involved in the initial illegality," the Court also refuted the

---

based on relative warmth—black is cool, white is hot, shades of gray connote relative differences. *Id.*

120 *Id.* at 29. The government suspected that the unusually high amounts of heat came from high-intensity lamps, which are required for indoor marijuana growth. *Id.*

121 *Id.* at 30. Based on tips from informants, utility bills, and the thermal imaging, a federal magistrate judge issued a warrant authorizing a search of the suspect's home. *Id.*

122 *See id.*

123 *Id.* at 41.

124 *Id.*

125 *Bartnicki*, 532 U.S. at 518.

126 *Id.*

127 *Id.* at 535.

128 *Id.* at 521. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, generally prohibits the intentional disclosure of illegally intercepted communication, which the disclosing party knows or should know was illegally obtained. 18 U.S.C. § 2511(1)(a), (c) (1994).

129 *Id.* at 534.

government's argument that punishing the radio station would serve the interest in removing an incentive for parties to intercept private conversations.[130]

It may be unwise to conclude, based only on a few cases, that the United States Supreme Court has demonstrated a clear and unwavering trend of favoring individual privacy over government surveillance. However, these cases do illustrate that the Supreme Court is adept at applying Constitutional jurisprudence to the new challenges brought by electronic surveillance, and that the Court will closely scrutinize the government's alleged justified surveillance in each case under the First and Fourth Amendments.

C. *United States v. Scarfo – The First District Court Case Involving the Legality of Key Logging Systems*

A final case that merits discussion is the *Scarfo* case.[131] According to the District Court of New Jersey, the case "presents an interesting issue of first impression dealing with the ever-present tension between individual privacy and liberty rights and law enforcement's use of new and advanced technology to vigorously investigate criminal activity."[132] The case "takes on added importance in light of recent events and potential national security implications."[133]

In *Scarfo*, the court had to determine whether the use of a "key logging" device by the FBI violated the Fourth Amendment rights of a suspect.[134] In order to decrypt the suspect's computer files, the FBI installed, under a search warrant, a "key logging" device on the suspect's computer, which could obtain the suspect's passphrases by capturing his keystrokes made on the computer.[135]

The arguments centered around whether the use of the "key logging" device constituted an "interception" of "wire communications" within the scope of the federal wiretap statute[136] and if so, then whether the FBI needed a wiretap order and not simply a search warrant.[137] The

---

130 *Id.* at 529.

131 United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001).

132 *Id.* at 574.

133 *Id.*

134 *See id.*

135 *See id.* at 574.

136 Title III, 18 U.S.C. § 2510 (1994).

137 *See Scarfo*, 180 F. Supp. at 581.

defense argued that an "interception" had been conducted since Mr. Scarfo used the computer to access the Internet, and every keystroke entered when the defendant was accessing the Internet was also captured and a "wire communication" thus "intercepted."[138] The defense also alleged that the search warrants had not been properly issued because the warrants failed to satisfy the particularity requirement with respect to the area and items to be searched and/or seized.[139]

The court first held that the search warrant was properly issued in accordance with Fourth Amendment requirements.[140] According to the court, the fact that keystrokes other than the required passphrase were recorded does not make the warrant lose its particularity.[141] The court analogized this to a common situation where the investigators might not know the exact nature of the incriminating evidence that they are searching for until they come across it.[142] Hence, "no tenet of the Fourth Amendment prohibits a search merely because it cannot be performed with surgical precision."[143] Secondly, the court found that the use of a "key logging" device did not amount to an "interception" under the federal wiretap law, because the device had been configured not to capture the keystrokes whenever the computer modem was activated.[144]

---

138 *See id.* at 576.

139 *See id.* The Fourth Amendment states that "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." U.S. CONST. amend. IV. Where a search warrant is obtained, the Fourth Amendment requires "a certain modicum of particularity in the language of the warrant with respect to the area and items to be searched and/or seized." *Id.*

140 *Scarfo*, 180 F. Supp. at 578.

141 *Id.*

142 *Id.*

143 *Id.* (quoting United States v. Conley, 4 F.3d 1200, 1208 (3d. Cir. 1993)).

144 *Scarfo*, 180 F. Supp. at 581. Recognizing that Scarfo's computer had a modem and thus was capable of transmitting electronic communications via the modem, the FBI configured the key logging device to avoid intercepting electronic communications typed on the keyboard and simultaneously transmitted through the modem. *Id.* As Randall Murch, a Special Agent of the FBI working as Deputy Assistant Director of the FBI Laboratory Division's Investigative Technologies Branch, explained in the Murch Affidavit:

> The default status of the keystroke component was set so that, on entry, a keystroke was normally not recorded. Upon entry or selection of a keyboard key by a user, the KLS ["key logger system"] checked the status of each communication port installed on the computer, and, all communication ports indicated inactivity, meaning that the modem was not using any port at that time, then the keystroke in question would be recorded.

Id.

The court was very careful in its decision to balance individual privacy with effective law enforcement, particularly in view of rapidly advancing technology, wherein the court stated:

> [W]e must be ever vigilant against the evisceration of Constitutional rights at the hands of modern technology. Yet, at the same time, it is likewise true that modern-day criminals have also embraced technological advances and used them to further their felonious purposes. Each day, advanced computer technologies and the increased accessibility to the Internet means criminal behavior is becoming more sophisticated and complex. . . . As result of this surge in so-called "cyber crime," law enforcement's ability to vigorously pursue such rogues cannot be hindered where all Constitutional limitations are scrupulously observed.[145]

This comment of the District Judge as to the delicacy and difficulty of the balancing exercised in cases of electronic surveillance is reminiscent of similar opinions expressed by other judges in similar cases. In *Berger v. New York*,[146] the United States Supreme Court had stated that "indiscriminate use [of eavesdropping devices] in law enforcement raises grave constitutional questions... Few threats to liberty exist which are greater than those posed by the use of eavesdropping devices."[147] Similar judicial sentiments had already been expressed in *Katz*[148] and in Justice Brandeis' dissent in *Olmstead*.[149]

IV. Proposal for the Judiciary's New Roles in the Area of Electronic Surveillance

In a moment of crisis, Congress acted too quickly to reassure the American people by enacting the USA PATRIOT Act.[150] As Congress

---

145 *Id.* at 583.

146 Berger v. New York, 388 U.S. 41(1967) (holding that the New York statute, which authorizes a court to issue *ex parte* orders to the government for eavesdropping upon oath or affirmation that there is reasonable ground to believe that evidence of crime may be thus obtained, contains no requirement for particularity as to what specific crime has been or is being committed or place to be searched or conversations sought as required by the Fourth Amendment, and requires no showing of exigent circumstances, is too broad in its sweep, resulting in trespassory intrusion into constitutionally protected areas, and is violative of the Fourth and Fourteenth Amendments).

147 *Id.* at 56.

148 *See supra* p. 4.

149 *See supra* p. 5.

150 Gia Fenoglio, *Jumping the Gun on Terrorism*?, 33 NAT'L J. 3450 (2001). The USA PATRIOT Act was signed into law less than six weeks after the attacks. The short time

failed to safeguard people's civil liberties in its zeal to defend the nation's security, and the new electronic surveillance law is subject to the abuses by the government,[151] the judiciary becomes the last resort for innocent individuals to safeguard their fundamental liberties. Consequently, the judiciary must closely and carefully supervise the actions of law enforcement and intelligence communities as they begin to use the new rules, and stop the abuses accordingly.

The judiciary must also strictly enforce the use of the USA PATRIOT Act. The Act should be limited to genuine cases of terrorism in order to ensure that law enforcement does not collect information for pure domestic criminal activities under the guise of 'intelligence' gathering. The USA PATRIOT Act primarily permits criminal investigations to fall within FISA surveillance authority if "a significant purpose of the surveillance is to obtain foreign intelligence information."[152] Thus, the government could easily evade the heightened standard of probable cause required under Title III for criminal wiretaps. In *Chagnon v. Bell*,[153] the D.C. Circuit Court warned that "when the foreign agent exception is invoked to justify warrantless surveillance, court must be alert to the possible pretextuality of the claim."[154] Therefore, the court must determine whether there exists a "direct link between the wiretap target and a foreign interest as a justification for surveillance," and whether the surveillance was "reasonably intended to guard national security data from foreign intelligence agencies."[155] Moreover, in *United States v. Truong Kinh Hung*,[156] the Fourth Circuit Court specifically laid out the "primary test" for the foreign intelligence exception. The primary test stipulated that the government should be excused from securing a warrant only when the surveillance is conducted "primarily" for foreign intelligence reasons.[157]

---

period for consideration, coupled with the chaos on Capitol Hill due to anthrax contamination, all suggest that the legislators lacked the time and opportunity to deliberate on the law. *Id.*

151 *See supra* note 68, statement of Sen. Leahy.

152 USA PATRIOT Act § 218 (2001) (amending § 1804 (a)(7)(B) of FISA).

153 Chagnon v. Bell, 642 F.2d 1248 (D.C. Cir. 1980).

154 *Id.* at 1260.

155 *Id.* (quoting Halperin v. Kissinger, 606 F.2d 1192, 1204 (D.C. Cir. 1979)).

156 United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

157 *Id.* at 915; *see also supra* note 108.

While both of these cases were decided applying pre-FISA law,[158] their cautionary statement remains appropriate in light of the expanded surveillance authority granted by the "significant purpose" provision of the amended FISA to the Executive.[159] The judiciary in the future must closely and carefully supervise the government's actions and ensure that the government is not using the guise of 'intelligence' gathering to collect information for pure domestic criminal activities.

Although the Foreign Intelligence Surveillance Court of Review held that the "primary purpose" test is not supported by FISA, and that the government could use foreign intelligence information in a criminal prosecution,[160] it never denied that information for pure domestic criminal activities must not be collected under the guise of intelligence gathering.[161] The Court of Review's approval of the FBI's proposed minimization procedures does not suggest that the court forego its constitutional requirement for the FBI's pure domestic criminal investigations. Conversely, the court should continue a restrictive attitude on the minimization procedures, and make sure that regardless of the situation, the sharing and dissemination of foreign intelligence information occur only when it is absolutely necessary.

Moreover, the court should also exercise stronger judicial oversight in issuing warrant. Pursuant to FISA, once the Attorney General certifies the application of a federal officer, the surveillance request is "subjected to only minimal scrutiny by the courts."[162] However, since the USA PATRIOT Act primarily permits criminal investigations to fall within FISA surveillance authority, the court's oversight of FBI's surveillance on domestic criminal activities will be diminished as the government is increasing the types of court-ordered surveillance for domestic crimes under the guise of intelligence investigation. Consequently, the court must strengthen its oversight in warrant issuing and give a heightened scrutiny to the surveillance request.

While the court must exercise strict judicial oversight in warrant issuing and information sharing to ensure that law enforcement is not collecting information for pure domestic criminal activities under FISA,

---

158 The courts used pre-FISA law because the wiretaps in question were authorized before 1978, the year FISA was enacted.

159 USA PATRIOT Act § 218 (2001) (amending §1804 (a)(7)(B) of FISA).

160 *In re*: Sealed Case Nos. 02-001, 02-002, *supra* note 102, at 727.

161 *See supra* Part I.B.1. Information for pure domestic criminal activities is constitutionally required to be subject to Title III and meet probable cause requirement.

162 United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984).

it must also take measures to protect people's legitimate privacy expectations. As the USA PATRIOT Act authorizes intelligence agencies to intercept communications from the Internet,[163] including electronic mail and Web surfing, which far exceed the definition of pen register and trap and trace devices under FISA,[164] the judge issuing the warrant must also investigate the information to be obtained. Information in the subject line of an e-mail provides more information than a number dialed on a telephone. When surveillance reveals content, the court must give it a heightened scrutiny as the FBI agents are gaining significant access to communications of non-targets and to information that it is not permitted to access under the purported court order.

The court should also provide sufficient privacy protections to innocent third parties as roving wiretap authority is expanded to FISA.[165]

As the USA PATRIOT Act does not extend the "reasonable proximate" privacy protection[166] to FISA roving wiretap practices, innocent third parties' conversations are intercepted by the government even though the target is not actually using the phone or has already left the location. The court should require the privacy protections to these parties to uphold their legitimate privacy expectations.

Finally, the court should be on alert that constitutionally protected political activities are not subject to FBI surveillance. As the USA PATRIOT Act broadly defines "domestic terrorism" as activities that may include political dissent and activism,[167] the court should uphold the spirit of the First Amendment by protecting people's free speech and associational privacy rights.[168]

---

163 USA PATRIOT Act § 216(a) (2001); *see also supra* note 76.

164 *See supra* note 73. Previously, under FISA, a pen register or trap and trace order only required a telephone company to reveal the numbers dialed to and from a particular telephone. *Id.*

165 USA PATRIOT Act § 206 extends Title III's roving wiretap authority to FISA. *See supra* note 71.

166 A Title III roving wiretap allows law enforcement agents to only intercept those conversations when the agents reasonably believe the target is using a particular phone. *See supra* note 70.

167 USA PATRIOT Act § 802 (2001). *See supra* note 78.

168 Brandenburg v. Ohio, 395 U.S. 444, 447 (1969). The Supreme Court ruled that the First Amendment forbids government from passing laws that prohibit the advocacy of violence or illegal activity, unless such advocacy is intended to incite "imminent lawless action" and is likely to produce such action. *Id.*

IV. Conclusion

America has a long history of balancing the national security interests against the constitutionally protected freedom of the people. Although in a time of national crisis, certain liberties can be sacrificed in order to protect the country, the United States ceases to be a country of freedom and democracy if those liberties are lost forever.

In enacting the USA PATRIOT Act and the Attorney General's Guidelines, Congress and the Executive Branch overreached their power and provided tools to take away important civil rights. The USA PATRIOT Act allows the government far greater power to monitor the private telephone conversations of individuals suspected of purely domestic criminal activity, without demonstrating probable cause that a crime has been or is soon to be committed, under the guise of an 'intelligence' surveillance;[169] overhear private conversations of non-suspects permitted by the extension of roving wiretap authority to foreign intelligence investigations without proper privacy protections;[170] intercept communications from the Internet, including electronic mail and Web surfing, which far exceed the definition of pen register and trap and trace devices under FISA;[171] discourage political dissent by including the activities of unpopular political organizations within the newly created definition of "domestic terrorism";[172] and expand the sharing of sensitive information between intelligence agencies and law enforcement.[173]

Undoubtedly, many of the changes instituted by the USA PATRIOT Act will be challenged in the federal courts. As Congress failed to safeguard people's civil liberties in its zeal to defend the nation's security, the judiciary has become the last resort for the country to rectify this wrong. The judiciary must assume active roles in examining and supervising the changing laws of electronic surveillance to protect the nation and uphold the Constitution. The courts should be vigilant that although it is critical for the government to have access to the tools required to combat terrorism, it is just as important that we avoid destroying the Constitution in the process.

Several recent cases revealed that the courts are giving more

---

169 *See supra* text accompanying notes 65-68.

170 *See supra* text accompanying notes 69-72.

171 *See supra* text accompanying notes 73-77.

172 *See supra* text accompanying notes 78-79.

173 *See supra* text accompanying notes 80-82.

deference to the Executive Branch in its efforts to combat terrorism and prevent future events like those of September 11th. In the first open opinion in its twenty-four-year history, the FISA Court of Review struck down the FISA Court's decision, and held that the Justice Department's proposed use of the USA PATRIOT Act in its minimization procedures is constitutional.[174] In *Scarfo*, the court found that the government's use of a key logging device on the suspect's computer is lawful even though it captures keystrokes other than the required passphrase.[175]

While these court decisions demonstrate a well-balanced weighing process and the final results they reached are reasonable given that we are facing unprecedented security threats, we shall not forget that insufficiently checked executive power to conduct electronic surveillance is dangerous. The Church Committee Report[176] in the early 1970s has provided one of the best examples in this respect.

Fortunately, the United States Supreme Court's recent decision in *Kyllo*,[177] and a long line of other cases such as *Katz*,[178] *Keith*,[179] and *Berger v. New York*,[180] has held that the Executive Branch's discretion in electronic surveillance is not unlimited, and that the Court will not allow the government's abuses of its surveillance powers if people's constitutional rights are severely injured. Although the Court's decisions in the area of electronic surveillance are not always consistent, as shown by the conflicting results of *Kyllo* and *Bartnicki*,[181] the decisions do demonstrate that the Court has the resolve to highlight the constitutional role and protections in light of electronic privacy issues. It will scrutinize the government's alleged justified surveillance very closely in each case, and base its decisions on different factual situations.

This Note suggests that the judiciary assume a more active role in examining and supervising the changing laws of electronic surveillance,

---

174 *See supra* Part III.A.

175 *See supra* Part III.C.

176 FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, S. REP. NO. 94-755, 94th Cong., 2d Sess. (1976).

177 *See supra* pp. 22-23.

178 *See supra* pp. 5-6.

179 *See supra* pp. 6-7.

180 *See supra* text accompanying note 146.

181 *See supra* pp. 22-24.

and act as an independent check on executive authority. Specifically, the courts should give substantive meaning to the word "significant" when deciding whether to admit information obtained from FISA surveillance in a criminal proceeding. If the government were unable to carry the burden of showing that national security had been a "significant purpose" of a FISA surveillance, any evidence so tainted could be excluded. Also, the courts should ensure that regardless of the situation, the sharing and dissemination of foreign intelligence information to criminal investigators and prosecutors occur only when it is absolutely necessary. This will further ensure that law enforcement is not collecting information for purely domestic criminal activities under the guise of an 'intelligence' surveillance.

In addition to a stronger judicial oversight in warrant issuing and information sharing, the courts should also take measures to protect people's legitimate privacy expectations through the surveillance period. The courts should investigate the information to be obtained by the FBI through the Internet and give it heightened scrutiny as it reveals more content than a number dialed on a telephone.[182] Also, the courts should require the privacy protections to innocent third parties as the USA PATRIOT Act does not extend the "reasonable proximate" privacy protection to FISA roving wiretap practices.[183]

Finally, the courts should be on alert that constitutionally protected political activities are not subject to FBI surveillance. The courts should adhere to a restrictive meaning of the definition of "domestic terrorism,"[184] and make sure that political dissent and activism are not included.

Nothing in this Note should be interpreted as suggesting that Congress should have never made those changes in the preexisting wiretap laws. As the country is facing unprecedented security emergencies, Congress had to make it easier for the government to combat terrorism and protect national security. This Note merely seeks to emphasize that before Congress could immediately incorporate any improvements into the USA PATRIOT Act, courts should assume a more active role in checking the Executive Branch and therefore, make it possible to both protect national security and provide greater protection for privacy than currently exists.

---

182 *See supra* text accompanying notes 73-77.

183 *See supra* text accompanying notes 69-72.

184 *See supra* note 78.