White Paper on The USA PATRIOT Act's "Roving" Electronic Surveillance Amendment to the Foreign Intelligence Surveillance Act

By

Peter M. Thomson
April, 2004

The Federalist Society
for Law and Public Policy Studies

The USA PATRIOT Act's "Roving" Electronic Surveillance Amendment to the Foreign Intelligence Surveillance Act

By Peter M. Thomson*

Introduction

For nearly two decades, commencing shortly after the advent of commercial cellular telephone service in the United States, federal law enforcement officers have had the authority, subject to court approval, to conduct "roving" wiretaps and electronic surveillance on persons suspected of committing federal crimes. A roving wiretap, also called a "multipoint" tap, attaches to a particular subject who utilizes multiple telephones or communications devices, rather than to a particular telephone or device, as in the case of a conventional wiretap. A roving wiretap, therefore, allows law enforcement officers to "follow" a subject and lawfully intercept that person's communications with a single court order when the person's telephone (or other communications device) is subject to change, e.g., because he or she is moving from phone to phone to thwart (or with the effect of thwarting) detection,[1] regardless of the phone used when communicating.

Prior to roving wiretaps, law enforcement agents and federal prosecutors had to invest substantial time and resources in obtaining a separate wiretap order for each additional telephone used by a subject during an investigation. Unfortunately, and quite often, this resulted in a loss of valuable evidence through missed wiretap conversations relating to the criminal activity being monitored.

---

*Peter M. Thomson is an Assistant United States Attorney for the Eastern District of Louisiana, U.S. Department of Justice. The opinions expressed here are only his own and do not necessarily represent those of the U.S. Department of Justice.

[1] 18 U.S.C. § 2518(11)(b).

In October, 2001, in the wake of the catastrophic events of September 11, the President signed into law the USA PATRIOT Act,[2] which, in part, expanded law enforcement and foreign intelligence authority in several vital areas of electronic intelligence gathering in an effort to combat terrorism. One specific provision, Section 206 of the Act, modified the Foreign Intelligence Surveillance Act of 1978 (hereinafter "FISA")[3] by extending roving surveillance authority to federal counterintelligence officers engaged in domestic foreign intelligence and counterterrorism investigations.[4]

Thus, prior to Section 206 of the PATRIOT Act, a federal law enforcement officer could employ roving surveillance to gather evidence in a criminal investigation, but a federal counterintelligence officer seeking to collect foreign intelligence information under FISA could not. For example, an FBI agent assigned to the Criminal Investigative Division could employ roving surveillance under Title III[5] to gather evidence in a criminal investigation against a suspected drug trafficker or money launderer; however, an FBI agent assigned to the Counterintelligence Division could not employ the same roving surveillance technology under FISA to gather intelligence relating to an al-Qaida operative present in the United States who was planning to inflict mass casualties with a hijacked airliner.

---

[2] Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001)(amending divers sections of Titles 18, 47, and 50, U.S. Code)(hereinafter "PATRIOT Act" or "Act").

[3] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1811 (1994 & Supp. 1999), 8 U.S.C. § 1101 (2000), 47 U.S.C. §§ 605-606 (1994 & Supp. 1999)), amended by Intelligence Authorization Act for Fiscal Year 2000, Pub. L. No. 106-120, 113 Stat. 1606 (1999).

[4] PATRIOT Act § 206 (amending 50 U.S.C. § 1805(c)(2)(B)).

[5] Referring to the federal wiretap law governing electronic surveillance for law enforcement purposes. *See* Title III, *infra* note 9.

Unfortunately, the expanded roving authority under FISA pursuant to Section 206 has met with stiff but unmerited opposition by defense attorneys and civil libertarian groups, who fear that Congress may have overstepped its legal limits and infringed upon fundamental American liberties. Spotlighted by the national media in a swirl of controversy, critics argue that roving FISA wiretaps violate the Fourth Amendment; create a serious potential for abuse; constitute an impermissibly broad expansion of government powers; are unlawfully invasive; and allow the improper monitoring of innocent third parties, among other claims of Constitutional, legal and public policy improprieties.

Brief History of Roving Surveillance in the Law Enforcement Context

During the past century, with the exception of the Japanese invasion of Pearl Harbor and the disastrous events of September 11, 2001, Americans have been largely immune to catastrophic foreign-sponsored acts of war and terrorism at home. Intelligence estimates prepared by the FBI during the 1980s and 1990s, however, identified a growing trend toward more destructive terrorist attacks[6] evidenced, in part, by the bombing of the World Trade Center in 1993 and the domestically-sponsored bombing of the Oklahoma City federal building in 1995. These events prompted substantial modifications of our foreign counterterrorism laws, including the enactment of the Anti-Terrorism and Effective Death Penalty Act of 1996 (hereinafter "AEDPA").[7] The events of September 11, however, were cataclysmic in nature and scope, and,

[6] J. T. Caruso, Deputy Executive Assistant Director, Counterterrorism & Counterintelligence, FBI, *Testimony Before the House Subcommittee on National Security, Veterans Affairs, and International Relations on "Combating Terrorism: Protecting the United States"* (March 21, 2002).

[7] Anti-Terrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (1996).

accordingly, justifiably generated an even more comprehensive review by Congress, The White House, and Executive Branch agencies, resulting in additional revisions of our foreign counterterrorism and counterintelligence regulations, policies, and laws, including those related to the government's ability and capacity to electronically monitor hostile foreign agents and terrorists present in the United States. Accordingly, anti-terror legislation, together with commensurate funding, developed gradually over the past decades in response to a growing "trend," which culminated in a terrorist event of unprecedented scope and horror.

Meanwhile, in the parallel context of federal law enforcement, and beginning in the 1960s, anti-crime legislation and funding mushroomed as the nation was engulfed in proliferating waves of organized crime, violence and drugs. Therefore, and quite understandably, domestic electronic surveillance legislation was directed to a greater degree over the past several decades toward investigating and prosecuting criminals and organized crime groups, including, e.g., Central and South American drug cartels, racketeering and money laundering organizations, the American "La Cosa Nostra," together with other emerging groups such as the Russian Mafia, Asian organized crime and violent street gangs.

In response to law enforcement's assertion that wiretaps were necessary to fight crime, combined with two landmark U.S. Supreme Court decisions[8] relating to federal wiretap authority, in 1968 Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act.[9] In an effort to protect privacy, Congress established within Title III a uniform legal procedure for conducting electronic surveillance in domestic criminal investigations.[10] Among

---

[8] *Berger v. New York*, 388 U.S. 41 (1967); *Katz v. United States*, 389 U.S. 347 (1967).

[9] Omnibus Crime Control and Safe Streets Act of 1968, Title III, Pub. L. 90-351, 82 Stat. 212 (June 19, 1968)(codified as amended at 18 U.S.C. §§2510-22) (hereinafter "Title III").

[10] *See* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the*

numerous other prerequisites to obtaining an intercept order, Title III required that each wiretap application: (a) include a specific description of the nature and location of the "facilities" from which or the place where the communication is to be intercepted; and (b) establish probable cause to believe that the "facilities" are being used, or are about to be used, in connection with the crime that is the focus of the surveillance.[11]

However, Title III was crafted for the then state-of-the-art in personal communications, the rotary telephone, a stationary device that allowed communications over "hard" wires, commonly referred to in law enforcement parlance as a "landline." Wiretaps were often accomplished by placing a pair of "alligator clips" over the wire posts that connected to the specific line used by the subject of the investigation. During the years following Title III's enactment, however, the nation witnessed a rapid if not explosive transformation in the technology of personal electronic communications that was certainly not foreseeable by the framers of the Constitution, particularly in the context of the Fourth Amendment.

Hence, approximately fifteen years after passage of Title III, portable analog cellular telephones became widely available, and "[b]y the mid-1980s, advances in telecommunications technologies presented new concerns not addressed by Title III."[12] Accordingly, in 1986 Congress recognized the need for additional legislative reform and updated Title III to cover the burgeoning technologies, including wireless devices, electronic mail, voice-mail and other advancements in communications technology.[13] The relevant 1986 amendments to Title III were

---

Federal Wiretap Laws to Enhance Privacy, 8 Alb. L. J. Sci. & Tech. 65, 71 (1997).

[11] 18 U.S.C. § 2518(1)(b)(ii) & (3)(d).

[12] Laurie Thomas Lee, *The USA PATRIOT Act and Telecommunications: Privacy Under Attack*, 29 Rutgers Computer & Tech. L. J. 371, 373 (2003).

[13] The Electronics Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat.

an attempt "to bring [the] new technologies ... into the statutory framework of the laws governing wiretaps."[14]

"Roving" Wiretap Authority

As amended by Congress in 1986, Title III granted law enforcement officers for the first time the authority to "follow" a suspect who purposefully switches telephones or other communications devices in an attempt to thwart electronic surveillance. Under the new roving surveillance provision, law enforcement had to demonstrate that a subject possessed the "intent" to thwart surveillance as a prerequisite for securing a wiretap order from a neutral and detached judicial officer. Thus, the amendment authorized investigators, under highly specific circumstances, to obtain a roving or multipoint wiretap or oral intercept order without having to specify the telephone or "facility" to be tapped in advance of the authorization.

The United States Court of Appeals for the Ninth Circuit explained the 1986 amendment to Title III, in the context of the rapid advances in cellular communications technology, as follows:

> Under the [new] provision, the government may obtain authority to intercept communications to and from any cellular phone number used by the target of an investigation. Before obtaining such authority, the government must establish that the target would thwart detection from a specified facility or location. When the government makes such a showing, it need not specify a particular communications facility or location at which the surveillance will take place and § 2518(1)(b)(ii) and (3)(d) do not apply. By enacting that provision, Congress 'contemplate[d] the roving surveillance of suspects who move from room to room in a hotel or of alleged terrorists who use different telephone booths to avoid surveillance.'[citation omitted] Roving wiretaps are an appropriate tool to investigate individuals, such as ... [the defendant], who use cloned cellular phone numbers and change numbers frequently to avoid detection. The roving wiretap

---

1848 (codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2709, 3121-3127 (2000)).

[14] Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception,* 34 Harv. J. on Legis. 393 (1997).

> provides the government with ample latitude to cope with the unique characteristics of cellular technology.[15]

The technological evolution, however, continued subsequent to 1986 at what seemed to be an even faster pace, and soon came the dawn of the digital age. Persons began communicating routinely over highly-portable and relatively inexpensive digital cell phones, the Internet, and other advanced personal communications devices such as wireless laptops, two-way paging devices, and "Blackberries." These advances, together with the advent of pre-paid dialing cards and Internet-friendly cell phones, created even more difficulties in attempting to monitor a person who deceptively elects to switch communications devices in a calculated effort to avoid surveillance. Moreover, the requirement of demonstrating a target's intent to defeat surveillance had created unforeseen and unnecessary impediments to roving wiretap investigations,[16] particularly in the context of the technological boom. Consequently, "intent" to thwart was often difficult to prove in advance of obtaining a roving wiretap order.[17] Thus, for example, prior to obtaining a roving wiretap order law enforcement officers were practically required to overhear a suspect admit (e.g., by means of a conventional wiretap or consensual monitoring) that he intended to use different telephones in an effort to defeat surveillance.[18] Further, on some occasions "[i]t may be that a subject moves from phone to phone ... because of

---

[15] *United States v. Hermanek*, 289 F.3d 1076, 1087 (9th Cir. 2002).

[16] *See, e.g.,* James P. Fleissner, Assistant Professor of Law, Mercer University, School of Law, *Testimony Before the Committee on the Judiciary, U.S. House of Representatives, on "The Comprehensive Antiterrorism Act of 1995"* (June 12, 1995) ("Requiring proof that the person to be intercepted has an intent to thwart intercept is unwise.").

[17] *See* Conf. Rep. on H.R. 3694, Intelligence Authorization Act (October 7, 1998).

[18] *See* 142 Cong. Rec. S.3437 (daily ed. April 17, 1996)(statement of Sen. Biden)(discussing multipoint wiretaps).

constant movement to distribute narcotics,"[19] in which case the subject might be relying on multiple personally owned telephones, for example, or ones possessed by criminal associates. Congress therefore recognized that switching telephones or other communications devices by a target could be attributed to other reasons not addressable under the 1986 "intent" standard, and that requiring proof of intent was an impractical and far too rigorous standard for criminal investigators, particularly with regard to the wide availability and use of diverse communications devices.

The 1998 Modification

Accordingly, in 1998, Congress responded once again to the law enforcement community's needs and amended the roving provision to allow continued surveillance when the target person's conduct would have "the effect" of thwarting surveillance, thereby removing the more stringent standard requiring that the applicant demonstrate the subject has the "intent" to thwart surveillance.[20]

Section 2518 of Title 18, United States Code, now provides, in pertinent part, the following:

> (11) The requirements of [earlier subsections requiring a particular description of the nature and location of the telephone or other communications facility *and* that probable cause be shown that the relevant "facility" is being used for identified criminal purposes] do not apply if–
>
> * * *
>
> (b) in the case of an application with respect to a wire or electronic communication–
>
> * * *
>
> (ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is

[19] *See* Fleissner, *supra* note 16.

[20] Pub. L. 105-272, Title VI, §604 (a)(1) (Oct. 20, 1998)(amending 18 U.S.C. § 2518 (11)(b)(ii)).

probable cause to believe that *the person's actions could have the effect of thwarting interception from a specified facility* [emphasis added].[21]

The War Against Terrorism and the Critical Need for FISA "Roving" Surveillance Authority

Congress enacted the Foreign Intelligence Surveillance Act[22] a decade before roving wiretaps were first introduced in the criminal context. In doing so, it mandated that U.S. intelligence agencies and the FBI submit to judicial supervision of electronic surveillance related to domestic internal security and terrorism investigations. FISA established a classified special court to review electronic intercept applications comprised of seven United States District Court judges (drawn from different circuits) appointed by the Chief Justice of the United States.[23] Applications for FISA intercept orders were required to be approved by the Attorney General,[24] contain specific language identifying the proposed target of the surveillance,[25] and demonstrate probable cause that the target was either a "foreign power" or an "agent" of a foreign power.[26] The application also had to contain: a statement of proposed minimization procedures; a certification that the information sought was foreign intelligence information; a statement addressing the length of time surveillance was required; and, a certification that the information

[21] 18 U.S.C. § 2518(11)(b)(ii).

[22] FISA, *supra* note 3.

[23] The PATRIOT Act amended FISA to increase the number of federal district judges from seven to eleven, of whom no fewer than three shall reside within twenty miles of the District of Columbia. PATRIOT Act § 208 (amending 50 U.S.C. § 1803(a)).

[24] 50 U.S.C. § 1804(a).

[25] *Id.*

[26] 50 U.S.C. § 1804(a)(4).

sought could not be reasonably obtained by normal investigative techniques.[27] Most notably, for purposes of this discussion, FISA additionally required that "each of [the locations at which surveillance was to be conducted was] being used or [was] about to be used, by a foreign power or an agent of a foreign power."[28]

The arrival of September 11, 2001, however, has ushered in a new and foreboding era in the history of terrorism. The "Pandora's Box" of terror has finally been opened and we must now anticipate and defend attacks inside our homeland with weapons of mass destruction that have the potential to dwarf the casualties observed at the World Trade Centers, the Pentagon, and at the rural field in Pennsylvania.[29] Thus, U.S. intelligence agencies are not only faced with detecting and preventing the hijacking of airliners, but also with detecting, intercepting and preventing foreign sponsored terrorists from unleashing biological, chemical and portable nuclear weapons within our borders, all of which constitute a clear and present security threat to this nation.[30] In order swiftly and effectively to meet these daunting challenges, speed and secrecy are of the utmost importance.

Terrorists and hostile intelligence agents are highly trained, well equipped and substantially financed.[31] For example, they employ "fronts" to further their clandestine

---

[27] 50 U.S.C. § 1804(a).

[28] 50 U.S.C. § 1804(a)(4)(B).

[29] *See, e.g.,* Carson Mark, Theodore Taylor, Eugene Eyster, Willliam Maraman, and Jacob Wechsler, *Can Terrorists Build Nuclear Weapons?*, Nuclear Control Institute, Washington, D.C., available at http://www.nci.org/k-m/makeab.htm ; *see also* Dr. Bruce G. Blair, *What if Terrorists Go Nuclear?* available at http://www.cdi.org/terrorism/nuclear-pr.cfm.

[30] *See National Strategy to Combat Weapons of Mass Destruction, The White House* (December, 2002) (hereafter *"National Strategy"*); *also see* Caruso, *supra* note 6.

[31] *See 2002 International Narcotics Control Strategy Report (Section on Money Laundering and Financial Crimes), United States Department of State (hereafter "State Dept.*

activities, and they launder funds needed for their operations.[32] They have infiltrated this country, both as individuals and within multiple terrorist "cells."[33] Because of their closed operational structures and strong ties of loyalty, it remains extremely difficult to infiltrate their organizations with undercover assets.[34] Therefore, the ability to eavesdrop unhampered but legally on their secret communications is crucial to the intelligence community's antiterrorism efforts. In response to September 11 and the difficult challenges we now face, and subsequent to an evaluation of intelligence-gathering procedures, the USA PATRIOT Act made both significant and minor changes to well over a dozen different federal statutes pertaining to electronic surveillance, as well as to other laws relating to money laundering and immigration, for example. The changes in the law, specifically in the area of electronic surveillance under FISA, were an appropriate and measured legislative response to the extraordinary and heightened risks we now confront from extremist groups whose focus has shifted to inflicting mass

---

Report"); *see also The Year 2015: The CIA Report*, ABC News Nightline with Ted Koppel, Jan. 7, 2001; Gerald O'Driscoll, Jr., Brett Schaefer, and John Hulsman, *Stopping Terrorism: Follow the Money*, The Heritage Foundation (September 25, 2001), available at http://www.heritage.org/research/nationalsecurity/BG1479.cfm.

[32] *See State Dept. Report, supra* note 31*; see also The 2002 National Money Laundering Strategy, prepared by the United States Department of the Treasury*, available at http://www.ustreas.gov/press/releases/docs/monlaund.pdf.

[33] *See National Strategy* and Caruso, *supra* note 30*; see also* Larry A. Melfford, Assistant Director, FBI Counterterrorism Division, *Testimony Before the United States Senate, Terrorism, Technology and Homeland Security Subcommittee, on "The State of the Terrorist Threat Facing the United States"* (June 27, 2003).

[34] *See* Frank Gaffney, Former Assistant Secretary of Defense, *Statements During CNN's Talk-back Live, aired October 3, 2001,* available at http://www.cnn.com/TRANSCRIPTS/0110/03/tl.00.html.

casualties.[35] The Act's modifications also represent a formidable and necessary enhancement of our intelligence agencies' ability to detect, prevent, and neutralize acts of terrorism.

Section 206 of the USA PATRIOT Act

Prior to the PATRIOT Act, "an order from a FISA court authorizing electronic surveillance was required to direct a specified communications carrier to help set up the surveillance if so requested in the application for the order."[36] However, international terrorists and foreign intelligence agents operating clandestinely within our borders are sophisticated and well trained in the circumvention of wiretaps and other methods of electronic surveillance.[37] Like narcotics traffickers and members of organized crime groups, even "street-level" criminals, foreign terrorists and intelligence agents frequently change locations, accommodations and communications devices, such as cellular phones and Internet e-mail accounts, with the result of defeating the electronic surveillance employed against them.[38] Under such circumstances, and prior to the PATRIOT Act, intelligence agencies were constrained to amend the surveillance order and resubmit it to the FISA court for review and approval. "This was a tedious process and caused critical breaks in electronic surveillance coverage. It was terribly difficult to operate with

---

[35] *See* Caruso, *supra* note 6, at 1.

[36] Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post September 11, 2001*, 94 Law Libr. J. 601, 614 (2002).

[37] *See* George J. Tenet, Director of Central Intelligence, *Statement Before the Senate Select Committee on Intelligence on the "Worldwide Threat 2001: National Security in a Changing World"* (February 7, 2001); *see also* Steven Levy, *Did Encryption Empower These Terrorists?*, Newsweek Web Exclusive, available at http://www.msnbc.com/news/627390.asp?Osi=.

[38] For example, the September 11 suicide highjackers are known to have used publicly accessible Internet connections at multiple locations as well as over one hundred different pre-paid calling cards to communicate from various public telephones, cell phones, and land lines. *See* Robert S. Mueller, FBI Director, *Statement for the Record, Joint Intelligence Committee Inquiry* (September 25, 2002).

full knowledge of the activities of the terrorist under surveillance when he [or she] could move from phone to phone on a whim [as a result of the new communications technology]."[39]

Recognizing that communications intelligence of all types and in all venues is a critical element of this nation's counterterrorism effort, Congress passed Section 206 of the Act which appropriately and necessarily expands roving surveillance authority to FISA court orders. This amendment was long-awaited and applauded by the Justice Department and U.S. intelligence agencies, which prior to September 11 had made several pleas to Congress to modify FISA in such a manner that would accommodate the changing methods by which terrorists communicate. By enacting Section 206 of the Act, Congress therefore brought FISA up to date with preexisting roving wiretap authority previously granted in criminal investigations pursuant to 18 U.S.C. 2518(11)(b)(ii), thereby granting intelligence agencies the ability to react more flexibly in time-sensitive counterterrorism investigations.

Section 1805 (c) of Title 50, United States Code, as amended by Section 206, now provides the following:

> (c) **Specifications and directions of orders**
> An order approving an electronic surveillance under this section shall ...
> (2) direct –
>
> (A) that the minimization procedures be followed;
> (B) that, upon the request of the applicant, a specified communication or other carrier, landlord, custodian, or other specified person, *or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other person* [emphasis added], furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

[39] Robert M. Blitzer, *Domestic Intelligence Challenges in the 21st Century,* available at http://www.lexingtoninstitute.org/homeland/blitzer.pdf.

Accordingly, Section 206 now permits "the FISA court order to omit the names of individual carriers where the court finds that the 'actions of the target ... may have the effect of thwarting the identification' of the carriers."[40] This allows a more generic surveillance order to attach to a "person" rather than requiring a separate court order identifying each telephone, Internet or other communications carrier or provider whose assistance is needed as that same person migrates from facility to facility. Hence, the investigative agency can "simply present the newly discovered carrier, landlord, custodian, or other person with a more generic order issued by the Court and effect FISA coverage as soon as technically feasible."[41] This clearly facilitates "a dramatic improvement in the ability to investigate and pursue terrorists 'on the move' who are plotting criminal activities."[42]

Section 206 of the PATRIOT Act therefore seeks to "level the playing field" with well-financed and highly trained terrorists and spies by authorizing federal intelligence agents to seek and obtain court permission to use the same roving surveillance techniques in national security and terrorism investigations that have been used for years by law enforcement agents to investigate criminals. Therefore, Section 206 is a logical and critical extension of a valid, lawful and time-tested criminal investigatory technique to our nation's antiterrorism surveillance efforts.

---

[40] Pikowsky, *supra* note 36, at 614.

[41] Tom Gede, Montgomery N. Kosma and Arun Chandra, *"Developing Necessary and Constitutional Tools for Law Enforcement,"* Federalist Society White Paper on Antiterrorism Legislation: Surveillance and Wiretap Laws, p. 15 (November 2001), available at www.fed-soc.org.; *see also American Civil Liberties Union, et al. v. U.S. Department of Justice,* 265 F.Supp.2d 20, 23 (D.D.C. 2003).

[42] Gede, Kosma and Chandra, *supra* note 41, at 15.

Unwarranted Criticism of "Roving" Surveillance Authority Under FISA

Critics and opponents of Section 206 claim that roving FISA surveillance is highly invasive and thereby creates a serious potential for abuse. Some legal scholars have likewise denounced the practice, both in the Title III and FISA context, arguing that it constitutes a dangerous "broad expansion of power" that does not incorporate sufficient privacy protections to reduce the risk that innocent third party users might have their right to privacy violated.[43] One criminal defense advocate went so far as to say that roving authority is "not a power the government needs."[44]

The ACLU, likewise, maintains that roving intercepts are "not limited to the target and will lead to interception of many innocent conversations not involving the target."[45] This argument of "incidental surveillance" arises, in part, from the PATRIOT Act's elimination of the government's obligation to establish before a FISA court that a target has actually used or is using the device sought to be tapped.[46] The most common example given in support of the "incidental surveillance" argument is the following: If a terror suspect uses a computer to access the Internet at a public facility, such as a library, café, or school, and the government has

---

[43] *See, e.g.,* Nathan C. Henderson, *The PATRIOT Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications,* 52 Duke L. J. 179, 195 (2002).

[44] Leslie Hagen, National Association of Criminal Defense Lawyers, available at http://www.snapshield.com/www_problems/United_States/Federal%20Roving%20Wiretap%20Rules%20Loosened.htm.

[45] American Civil Liberties Union, *Surveillance Powers: A Chart*, at http://archive.aclu.org/issues/privacy/Patriot_Chart_law.html (Oct. 10, 2001); *see also* Elkan Abramowitz & Barry A. Bohrer, *In the Name of Counter-Terrorism*, N. Y. L. J., Nov. 6, 2003, at 6 (arguing a drastic increase of incidental surveillance).

[46] PATRIOT Act § 206, 115 Stat. at 282 (government must show target to "thwart" surveillance).

implemented a roving FISA wiretap order to monitor that person's communications, the surveillance agents might monitor all relevant Internet communications at the same site after the terror suspect has terminated the suspected communications.[47] Likewise, a public facility such as a library might have several computers and the surveilling agents may not know in advance which facility or facilities the terror suspect will use. In such case, agents might inadvertently or incidentally monitor communications over one or more computers used by third persons who are not made subject of the surveillance order.

Consequently, the ACLU and other critics maintain that roving surveillance violates the Fourth Amendment's "particularity" requirement. Under the "Fourth Amendment, a warrant must specify the place to be searched in order to avoid random searches of innocent bystanders."[48] "In the context of electronic surveillance," civil libertarians and some scholars argue, "the Constitution should therefore require ... [federal] officers applying for a court order to specify the phone [or computer or other facility] they want to tap."[49] Otherwise, "the back door to massive wiretapping" might be opened.[50]

---

[47] American Civil Liberties Union, *How the Antiterrorism Bill Limits Judicial Oversight of Telephone and Internet Surveillance*, at http://www.aclu.org/congress/1102301g.html (Oct. 23, 2001); *see also* Patricia Mell, *Big Brother at the Door: Balancing National Security With Privacy Under the USA PATRIOT Act*, 80 Denv. U. L. Rev. 375,423 (2002).

[48] Jim McGee, *An Intelligence Giant in the Making: Antiterrorism Law Likely to Bring Domestic Apparatus of Unprecedented Scope*, WASH. POST, Nov. 4, 2001, at A04.

[49] Lee, *supra* note 12, at 396. Although the government does not have to establish actual "use" of a phone or other device prior to obtaining an order, it must nevertheless establish by specific allegations that actions by the target may have the effect of circumventing the tap. If the government fails to make such a necessary showing to a reviewing FISA court judge, the issuance of a roving order is not legally permitted. *See* 50 U.S.C. § 1805(c)(2).

[50] Carrie Kirby, *Watchdogs Say Terror Bill Goes Too Far*, S. F. CHRON., Oct. 25, 2001, at D1; *see also* Lee, *supra* note 12, at 396.

The critics' account is unsatisfactory for a number of reasons. To begin with, the Fourth Amendment's reasonableness requirement does not apply to national security investigations in the same way it applies in criminal cases. The Fourth Amendment protects against "unreasonable searches and seizures."[51] In the law enforcement context, a search is presumptively unreasonable unless conducted pursuant to a warrant.[52] Courts have stated and legal scholars have opined, however, that electronic surveillance conducted for national security purposes by the Executive is likely exempt from the Fourth Amendment–or at a minimum the warrant requirement does not apply–particularly in cases involving foreign powers and their agents.[53]

Notwithstanding such an exemption, however, a different standard of "reasonableness" under the Fourth Amendment is invoked in a national security setting than in a criminal law context.[54] The Supreme Court has recognized that "domestic security surveillance may involve different policy and practical considerations from the surveillance of 'ordinary crime.'"[55] Thus, "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both

---

[51] U.S. Const. Amend. IV.

[52] *See id.* (providing 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."); *see also Camara v. Mun. Court*, 387 U.S. 523, 534 (1967).

[53] *See, e.g., United States v. Duggan*, 743 F.2d 59 (2d Cir. 1984)(citing cases); *United States v. Truong Dinh Hung*, 629 F. 2d 908, 914 (4th Cir. 1980); *United States v. Butenko,* 494 F.2d 593 (3d Cir. 1974)(en banc); *United States v. Brown,* 484 F.2d 418 (5th Cir. 1973); *cf. United States v. Usama Bin Laden,* 126 F. Supp. 2d 264 (S.D.N.Y. 2000). For further discussion about the national security exemption, *see generally* David Hardin, *The Fuss Over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA Under the Fourth Amendment*, 71 Geo.Wash. L. Rev. 291 (2003).

[54] *See United States v. United States Dist. Court,* 407 U.S. 297 (1972).

[55] *Id.* at 322.

in relation to the legitimate need of [g]overnment for intelligence information and the protected rights of our citizens."[56] Accordingly, any determination of "reasonableness" within the meaning of the Fourth Amendment in a national security context should balance (a) the duty of the government to protect against national security threats with (b) the dangers to individual privacy interests posed by the relevant electronic surveillance procedure.[57]

Regardless, even if one accepts the proposition that FISA surveillance can lead to Fourth Amendment violations, such as an "incidental" intercept during a roving wiretap at a library, the available remedy is a case by case exclusion of the conversations or other evidence seized by virtue of the roving surveillance order. Therefore, if FBI agents employing FISA surveillance obtain evidence against a non-targeted party that leads to criminal prosecution, the aggrieved defendant retains the right to file a motion to suppress the evidence acquired during the FISA surveillance.[58]

In the context of Title III, a number of federal appellate courts have previously held that roving wiretaps do not violate the particularity requirement.[59] Thus, "the safeguards required by congress provide adequate protection to preserve the constitutionality of interceptions of oral conversations when authorized under 18 U.S.C. § 2518(11)(a)." [60]

---

[56] *Id.* at 322-23.

[57] *Id.* at 314-15; *see also In re Sealed Case,* 310 F.3d 717, 742 (Foreign Int. Surv. Ct. Rev. 2002)(concluding FISA constitutional under Fourth Amendment and that the particularity requirement is satisfied by designating the type of intelligence sought and by certifying that said information is foreign intelligence information); *Whren v. United States,* 517 U.S. 806, 818 (1996).

[58] 50 U.S.C. § 1806; *see, e.g., United States v. Cavanagh*, 807 F.2d 787 (9th Cir. 1987).

[59] *See Hermanek, supra* note 15; *see also United States v. Bianco,* 998 F.2d 1112 (2d Cir. 1993); *United States v. Gaytan*, 74 F.3d 545 (5th Cir. 1996); *Petti, infra* note 61.

[60] *Bianco, supra* note 59, at 1124.

The Ninth Circuit spoke directly to the issue (in the context of Title III) in *United States v Petti,*[61] reasoning that the particularity requirement of the "place" to be searched may be substituted with that of the "person" in a roving wiretap setting. Thus, a roving order authorizing a wiretap over all telephones used by a subject does particularly describe the "places" or telephones to be searched, albeit in an unconventional manner, in that only those *specific* telephones (or computers, etc.) used by *that* subject may be tapped. The court noted that the government still has the corresponding obligation to minimize all calls, and that Title III only allows a roving order "if the government establishes to the court's satisfaction that it is impossible to specify the facilities because it is the suspect's purpose to thwart interception by changing them."[62] In concluding that roving wiretaps satisfy the Fourth Amendment's particularity requirement, the Court reasoned that roving surveillance permits no greater invasion of privacy than is necessary to meet "the legitimate needs of law enforcement."[63] The above rationale as adopted by the Ninth Circuit is undoubtedly based, in part, on the Fourth Amendment's adaptable reasonableness standard, particularly with regard to advances in technology that were not foreseeable by the founding fathers.[64]

Although the Supreme Court has yet to specifically address the roving wiretap debate in either the FISA or Title III context, it would appear that the appellate decisions upholding the constitutionality of roving surveillance are based on solid legal ground, particularly when the

---

[61] *United States v. Petti,* 973 F.2d 1441 (9th Cir. 1992), *cert. denied,* 507 U.S. 1035 (1993).

[62] *Id*. at 1445.

[63] *Id.* (*citing, Katz v. United States,* 389 U.S. at 355-56).

[64] *See* Akhil Reed Amar, *Fourth Amendment First Principles,* 107 Harv. L. Rev. 757, 802-810 (1994).

President's Constitutionally-imposed duty to protect national security is considered. Fourth Amendment limitations on government authority are most likely not exceeded for this reason as well "because the threat to privacy ... appears to be outweighed by the government's duty to protect national security."[65] Hence, prior to and after the enactment of FISA, courts have recognized the President's intrinsic authority to conduct surveillance in furtherance of national security,[66] as it is recognized that "no government interest is more compelling than the security of the Nation."[67]

Moreover, Congress intentionally built into FISA strict certification, oversight and minimization procedures, in addition to the other procedural criteria outlined above that must be followed by federal officers in surveillance applications, roving or non-roving. For example, FISA requires certifications from high-ranking officials within the Executive Branch, such as the President's National Security Advisor, the FBI Director or other similar official,[68] attesting that a "significant purpose"[69] of the proposed surveillance is to obtain "foreign intelligence

---

[65] *See United States v. U.S. District Court*, 407 U.S. at 315; *see also* Henderson, *supra* note 43, at 198; U.S. Const. art. I, § 7, cl. 15 and art. II, § 1, cl. 8.

[66] *See, e.g., United States v. Butenko, supra* note 53, at 608; *United States v. Truong Dinh Hung*, *supra* note 53, at 914. For a more comprehensive discussion, *see Supplemental Brief for the United States, In Re [deleted], in the U.S. Foreign Intelligence Surveillance Court of Review,* No. 02-001, at http://www.fas.org/irp/agency/doj/fisa/092502sup.html, at 18.

[67] *Haig v. Agee*, 453 U.S. 280, 307 (1981); *see also U.S. Supp. Brief,* at 21.

[68] 50 U.S.C. § 1804(a)(7); *see also* Exec. Order No. 12139, 44 Fed. Reg. 30311 (May 23, 1979) delineating the following Executive Branch Officials: Secretary of State; Secretary of Defense; Director of Central Intelligence; Director of the FBI; Deputy Secretary of State; Deputy Secretary of Defense; and, Deputy Director of Central Intelligence. These officials are authorized under the Executive Order only if appointed by the President and confirmed by the United States Senate.

[69] Prior to the PATRIOT Act, the government was required to establish that the *primary* purpose was to obtain foreign intelligence information. *See* § 218 of the USA PATRIOT Act, Pub. L. N. 107-56, 115 Stat. 272, 291 (2001). The "primary purpose" requirement may have

information"[70] that cannot be reasonably obtained by normal investigative techniques.[71] Further, the Attorney General or Deputy Attorney General[72] must approve every FISA application prior to submission.[73] The FISA application process therefore assures that the highest Executive Branch officials are held personally accountable for the electronic surveillance that they authorize.[74] Likewise, roving FISA wiretap orders must be approved and issued by a neutral Article III judge who has been designated by the Chief Justice to serve on the FISA Court. This assures that intelligence agencies' domestic surveillance activities are made fully subject to judicial review.[75]

---

contributed to the failure of U.S. counterintelligence officers to detect and thwart the September 11 attacks. *See* David Johnston & Philip Shenron, *FBI Curbed Scrutiny of Man Now a Suspect in the Attacks*, N.Y. Times, Oct. 5, 2001, at A1 (alleging that the FBI refrained investigating Zacarias Moussauoui, after learning that he desired to fly jetliners without landing instructions, based on ground that pursuing criminal case might lend future difficulty to obtaining FISA surveillance order). The new standard should permit better coordination between law enforcement and foreign intelligence-gathering investigations involving criminal activity such as, for example, terrorism and sabotage, that are inextricably intertwined with hostile activities of foreign powers or their agents.

[70] "Foreign intelligence information" means, generally, information concerning foreign-sponsored acts of sabotage or terrorism, as well as clandestine intelligence activities or the attack or planned attack by a foreign power against the United States. *See* 50 U.S.C. § 1801 (e).

[71] *See* 50 U.S.C. § 1804 (a)(7)(A-E) for entire list of required certifications.

[72] The Deputy Attorney General "is authorized to exercise all the power and authority of the Attorney general, unless any such power or authority is required by law to be exercised by the Attorney general personally." 28 C.F.R. § 0.15(a) (2000).

[73] 50 U.S.C. § 1804 (a).

[74] *See Bianco, supra* note 59, at 1124.

[75] Although critics counter that few FISA applications are rejected, it is notable that the ratio approximates Title III. *See "The Nature and Scope of Government Electronic Surveillance Activity," infra* note 96. Moreover, the authorization process within the Department of Justice for FISA wiretap orders is even more rigorous than that required for Title III orders. Consequently, only the most legally and factually compelling FISA wiretap applications are approved for submission to the FISA court.

FISA surveillance is also subject to substantial Congressional oversight. The Executive Branch must keep the Congressional Intelligence Committees "fully inform[ed] ... concerning all electronic surveillance" under FISA.[76] In fact, "Congress has made it clear its intention to hold the Executive Branch accountable for the exercise of its FISA authority."[77]

Although FISA does not incorporate minimization requirements as strict as Title III, the minimization provisions nevertheless do require minimization of conversations of "U.S. persons."[78] FISA requires that agencies only intercept "material relating to the target and to the [foreign intelligence information] with the least intrusion possible."[79] Furthermore, FISA requires that information concerning a U.S. person not be retained or disseminated *unless* it is "foreign intelligence" or evidence of an ordinary crime, which may be shared as necessary and appropriate with law enforcement officers.[80]

Section 206 critics also maintain that the standard of proof for a FISA roving wiretap is substantially less onerous than that required for a roving tap in a criminal context. Hence, "[a] multipoint wiretap, covering every phone that a target might use, may be obtained based [simply] on the 'probable cause that the target is a foreign power or agent of a foreign power.'"[81] Thus,

---

[76] 50 U.S.C. § 1808(a).

[77] *See* § 224(a) of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[78] 50 U.S.C. § 1801(h)(1).

[79] Gerald Robinson, *We're Listening! Electronic Eavesdropping, FISA, and the Secret Court*, 36 Willamette L. Rev. 51, 65 (2000).

[80] *See* 50 U.S.C. §§ 1801(h) & 1806.

[81] 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, 481 (2002).

these critics decry the PATRIOT Act's extension of roving authority to "terrorist probes ... [because it eliminates] the probable cause requirement [embodied in Tile III]."[82]

At this juncture it is important to underscore an obvious but significant and defining distinction between FISA and Title III. FISA regulates the collection of foreign *intelligence* information relating to terrorism plots, espionage, sabotage, and planned assassinations, for example. Title III, on the other hand, regulates the collection of *evidence* to be used in a *criminal* prosecution. Thus, attempts to apply an identical probable cause standard upon these two constitutionally distinguishable and distinct areas of government responsibility is inappropriate and misleading.

Thus, whereas Title III requires a showing of probable cause that a predicate crime is being committed and that the subject named in the wiretap order is committing the crime or will commit the crime over the phone to be tapped, FISA requires the court to review the government's application and make a finding that "there is *probable cause* [emphasis added] to believe that ... the target of the electronic surveillance is a foreign power or an agent of a foreign power: provided, [t]hat no United States Person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States."[83] Accordingly, FISA restricts its wiretap authority to monitoring "foreign powers" or their "agents" including "United States persons" for the specific purpose to obtain national security information.[84] The definition of "foreign power" includes

[82] Lee, *supra* note 12, at 396.

[83] 50 U.S.C. § 1805(a)(3).

[84] 50 U.S.C. § 1804(a)(1)-(6); *see also* Bradley, *supra* note 81, at 472.

foreign governments and terrorist groups.[85] Therefore, while FISA demands less of a nexus between the device and relevant communications, it requires more of a nexus between the targeted communications and subject of the surveillance.[86] Accordingly, the "probable cause" standard for FISA is appropriately tailored to the national security context and for the express purpose of garnering foreign intelligence.

The ACLU has suggested that FISA wiretaps pose a greater challenge to privacy because they are authorized secretly without a showing of probable cause of a crime.[87] However, to obtain a FISA wiretap against a U.S. citizen (or a Lawful Permanent Resident of the United States), the government must also establish that the activities involve or may involve a violation of federal criminal law.[88] Thus, when a U.S. citizen is named or described as a target of FISA surveillance and is, accordingly, acting as an "agent of a foreign power," probable cause must exist to justify belief that the person is engaged in an activity that involves or is about to involve a violation of federal criminal law, including espionage, terrorism, sabotage, use of fraudulent identity, or conspiracy.[89] Furthermore, each FISA application must certify that a significant purpose of the surveillance is to obtain foreign intelligence information, defined, in part, as information that is necessary (concerning a U.S. citizen) to defend against foreign attack or the crimes of terrorism, sabotage, or espionage.[90] Accordingly, with regard to a "United States

---

[85] 50 U.S.C. § 1801 (a).

[86] *See* H.R. Rep. No. 95-1283, Part I, 95th Cong., 2d Sess. 15-22 (1978).

[87] ACLU, *How the USA-PATRIOT Act Limits Judicial Oversight of Telephone and Internet Surveillance*, at http://archive.aclu.org/congress/l102301g.html.

[88] 50 U.S.C. § 1801(b)(2).

[89] *Id.; See also* 50 U.S.C. § 1804(a)(4).

[90] 50 U.S.C. § 1801(e).

person," or in certain instances non-citizens, the establishment of probable cause that the target is an agent of a foreign power contemporaneously establishes probable cause that the person is engaged in (or about to be engaged in) a violation of federal criminal law.

There are a number of additional reasons that serve to refute the claims of Section 206 critics that roving surveillance impermissibly threatens individual liberty and privacy interests. First, there is nothing in Section 206, much less the entire PATRIOT Act, which serves to vitiate or surrender any of the rights, privileges and immunities guaranteed to American citizens under the Constitution. To the contrary, FISA specifically and affirmatively seeks to protect and preserve the inalienable rights guaranteed to American citizens, as well as to aliens lawfully admitted for permanent residence.[91] As noted earlier, FISA states that "no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States."[92] Thus, a U.S. citizen (or even an alien admitted for permanent residence) cannot be made the target of an electronic surveillance order solely on the basis of activities secured by the First Amendment. Second, the potential for abuse of power with roving surveillance inheres in any government power. However, the Supreme Court repeatedly has reminded us that the law presumes good faith government conduct.[93] The more relevant focus should be whether sufficient checks and balances exist within the present FISA framework to manage and contain that power. Clearly, sufficient certifications and safeguards do exist–including those of judicial review and Congressional oversight–and the internal security benefits of allowing roving wiretaps outweigh

[91] *See* 50 U.S.C. § 1805 (a)(3)(A).

[92] *Id.*

[93] *See, e.g., United States v. Mezzanatto,* 513 U.S. 196, 210 (1995).

the risks, including the inherent risks of taking no action whatsoever. Third, roving wiretaps are used infrequently. Although the occurrence of roving FISA wiretaps remains classified,[94] an analogy can be made with Title III where roving taps are extraordinarily rare. Within the last year, for example, only several roving Title III wiretap orders (applicable to electronic devices) were granted on the federal level. In fact, between 1999 and 2002, just over 1,000 wiretap orders (federal and state) were granted annually of which, in 2002 for example, only nine (three federal and six by State authority) were roving.[95] Likewise, based on a 2001 report, FISA typically issues just over 1,000 electronic intercept and search orders on an annual basis.[96] Although the number of roving authorizations is unknown, it is logical to assume that the frequency would comport with the use of similar surveillance in a criminal context where both criminal suspects and counterintelligence targets have access to the same roving-allowable communications technology.

Critics, however, may argue that if roving technology is seldom used, then why grant intelligence agencies the power in the first place, as the benefits would certainly be outweighed by the risks to personal liberties. However, the more fundamental question in such a case relates not to frequency, but to strategic importance. Hence, it is critical to our nation's antiterrorism

---

[94] Details concerning the use of Section 206 were provided to the House Permanent Select Committee on Intelligence on May 29, 2003, in response to a request by the House Committee on the Judiciary.

[95] 2002 Wiretap Report, Administrative Office of the United States Courts, available at http://www.uscourts.gov/wiretap02/table2-02.pdf.

[96] *The Nature and Scope of Government Electronic Surveillance Activity,* www.cdt.org/wiretap/wiretap_overview.html (September 1, 2001). Since the terrorist attacks of September 11, 2001, however, FISA warrants (intercept and search orders) have increased by eighty-five percent to approximately 1,700 in 2003. Robert S. Mueller, III, FBI Director, *Testimony Before the National Commission on Terrorist Attacks Upon the United States* (April 14, 2004), available at: www.9-11commission.gov/hearings/hearing10/mueller_statement.pdf; *see also* related news story at www.msnbc.msn.com/id/4752004.

efforts that our intelligence agencies possess the legal capability to intercept all forms of communications utilized by terrorists and hostile intelligence agents. If "one" roving tap leads to the seizure of a large cache of botulism toxin in New York or a portable nuclear bomb in Los Angeles, have the benefits outweighed the risks to personal liberties? Moreover, how does the potential loss of privacy to persons over the Internet, for example, compare to the massacre of several thousand persons, the closure of international airspace, the utter destruction of skyscrapers in New York, an economy in a tailspin, and Americans living in terror and afraid to fly on commercial airliners?

The fact of the matter is that on September 11, 2001, the United States was drawn into an unconventional war against not only an organization, i.e., al-Qaida, but against an amorphous conglomerate of foreign-based Islamic extremist groups drawn together by a common radical ideology with the express aspiration of causing mass casualties of Americans. Such a conflict is unlike any other war this nation has ever fought. An intelligence failure, through one missed wiretap call, for example, could potentially lead to the deaths of thousands. Accordingly, technical superiority and the ability to conduct lawful "national security" electronic surveillance in all forms and venues are critical to this nation's effort to prevent domestic terrorism.

Final Comments on Recent
Efforts to Dilute FISA Roving Authority

Under current law, FISA requires that every surveillance order specify: (a) the identity, if known, or a description of the target of the electronic surveillance; and (b) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known.[97] Thus, FISA does not require that particular communications facilities be specified, nor

[97] 50 U.S.C. § 1805(c)(1)(A)-(B).

the target's identity, except that a "description of the target" must be provided *in all cases* where his identity is not known.[98]

The latter factual scenario, *i.e.*, a roving wiretap (unspecified facilities) where the target is not identified, has been referred to by commentators as the "John Doe" roving wiretap.[99] This inappropriate and somewhat misleading reference has created a discernable level of confusion in the public and media alike in that the label seems to infer that a roving wiretap order can be employed against *anyone* once issued. This is flatly wrong because a particular individual in all cases must nevertheless be *described* where his identity is lacking.[100]

Notwithstanding the sporadic confusion, however, roving wiretaps of "non-identified" targets have been decried by civil libertarians as a further encroachment on privacy interests, thereby setting the stage, in part, for recent efforts to rein in certain provisions of the PATRIOT Act perceived to have been hastily enacted and invasive to civil liberties.[101] Reform proponents want new and more restrictive limitations placed on the use of search warrants and electronic surveillance, including roving wiretaps under FISA. They argue that the government's ability to obtain "John Doe" roving wiretaps increases the likelihood that conversations of third parties unrelated to an investigation will be intercepted.[102] Likewise, they argue that the FISA roving

---

[98] 50 U.S.C. § 1805(c)(1)(A).

[99] *See* The Friends Committee on National Legislation ("FCNL"), "Legislation Action Message" (Oct. 9, 2003), available at: http://www.fcnl.org/act_lam_current/lam109_03.htm.

[100] 50 U.S.C. § 1805(c)(1)(A).

[101] *See* Center for Democracy & Technology, *CDT Urges Congress to Move Forward With Legislation to Fix the PATRIOT Act (Press Release)* (Jan. 13, 2004), available at: http://www.cdt.org/press/031014press.shtml; *see also* People for the American Way, *USA PATRIOT Act, Developments in the 108th Congress* (updated Oct. 28, 2003), available at: http://www.pfaw.org/pfaw/general/default.aspx?oid=9716.

[102] *See id.*; *see also* Tech Law Journal, *Bulletin: News From October 1 - 5, 2003,*

provision "constitutes a virtual blank check for wiretap surveillance permission."[103] In a recent letter to Congress, the ACLU stated that the "PATRIOT Act also contained an apparent error in that it allows roving wiretaps even if federal agents do not know who is the target or what telephone or device is being used."[104] The ACLU maintains that the law needs to be clarified "to require that federal agents know at least one of these two things to obtain a roving wiretap."[105] (Again, this characterization is inaccurate as agents must always provide a description of the target).

Therefore, opponents of the PATRIOT Act seek to have the law amended so that every FISA order must specify either (a) the target's identity, *or* (b) the facilities to be tapped *and* a description of the target. Thus, if the target is identified, then the facilities do not have to be specified and a roving order would be authorized. If the target cannot be identified, however, then the facilities must be described and a roving order under § 1805(c)(2)(B) would not be permitted. The ACLU also maintains that if the facility (place the surveillance will be directed) is unknown at the time of the order, the law should be revised so to allow surveillance only when the target is personally present at the facility or location.[106] Therefore, the ACLU and other opponents of FISA, as amended by the PATRIOT Act, seek to categorically prohibit the issuance of a roving order (to "such other persons" where the target's actions thwart surveillance) unless the order specifies the identity, *i.e.*, true name, of the target of the electronic surveillance.

---

available at: http://www.techlawjournal.com/home/newsbriefs/2003/10a.asp.

[103] *See* FCNL *supra*, note 99.

[104] American Civil Liberties Union, Legislative Update (Letter to the Senate, Oct. 8, 2003), available at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13993&c=206:

[105] *Id.*

[106] *See id.*

As reasonable and measured as these proposed restrictions may seem at first impression to some, if implemented they would have a deleterious effect on the government's domestic ability to investigate and prevent acts of espionage, sabotage and terrorism. Those advocating reform as described above apparently misunderstand the FISA statute that authorizes roving wiretaps as well as the potential factual scenarios that might play out during an actual terrorism or foreign counterintelligence investigation. A misconception also apparently exists with reform proponents regarding the logistics involved in implementing certain forms of electronic surveillance in rapidly developing situations where time is of the essence.

Requiring Proof of Identity for FISA Roving Authority Would Reward Terrorists

FISA provides that even if the "identity" of a target has not been confirmed by the government, the intercept order issued by the FISA court must nevertheless provide a "description of the target of the electronic surveillance."[107] Hence, a "virtual blank check" for surveillance does not exist in this regard. The government cannot run amuck and eavesdrop on any new target of its choosing. To the contrary, FISA at § 1805(c)(1)(A) explicitly requires that the order be directed toward a specific person, detailed by a description of that person, even though the person's true name and identity may not be discernable by FBI counterintelligence agents in advance of the application. In fact, it may be that the person's identity *is* the information sought, in part, by the surveillance.[108] Moreover, the government cannot, *sua sponte*, modify the target described in a roving FISA order once issued; an order directed against

[107] 50 U.S.C. § 1805(c)(1)(A).

[108] It is interesting to note that an "agent of a foreign power" includes any person who knowingly enters the United States with a fraudulent identity or who subsequently assumes a false identity (for or on behalf of a foreign power). *See* 50 U.S.C. § 1801(b)(2)(D). Thus, FISA recognizes that a target of electronic surveillance, including roving surveillance, may be operating already under an assumed identity.

one target cannot be employed against another without the government reapplying to the FISA court and obtaining a new order of electronic surveillance.

Although roving wiretaps may be used infrequently[109] where a target's "identity" is not known (but a description is available), under such circumstances a roving order may be an essential if not critical tool in tracking a terrorist or foreign agent. For example, a hostile agent might employ a pseudonym as a cover and thus be considered "unidentified," or a terrorist may have entered the country with a forged passport containing a false name and his identity cannot be determined in advance of a needed surveillance order which application is based on time-sensitive information. Moreover, because of increased security at border crossings, more terrorists might choose to be smuggled[110] into the United States under false identities. Accordingly, circumstances may undeniably develop in an investigation where a physical description of a terrorist (or other target) is known, but not his identity.

As a further example, imagine that during a time-sensitive investigation the FBI has only a physical description of a target who, according to information received, is planning an event such as possibly a terrorist attack or a secret meeting with other high-level operatives. The FBI may know where the target is temporarily residing, and that he is using public pay telephones and publicly accessible computers in the general vicinity to communicate with his associates. Special Agents may have followed him to locations where numerous computers are available for use by the general public, such as public libraries, Internet cafés and universities. They have observed him use several of these computer facilities on a random basis at multiple locations.

---

[109] The incidence of FISA roving wiretaps and supportive facts is classified national security information.

[110] *See* "PBS Frontline" Report, *Crossing Borders: How Terrorists Use Fake Passports, Visas and Other Identity Documents* (2001), available at: http://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html.

Additionally, the FBI may have confirmed that the target is using certain e-mail accounts,[111] but agents are unable to predict exactly what computer or account he may use next or where the facility will be located.

Under current law, the FBI can obtain a roving order that will authorize the monitoring of the computers or pay telephones that the target next utilizes subject to court-mandated minimization procedures. If the PATRIOT Act were amended as sought by the ACLU, for example, FISA would not authorize a surveillance order under the same scenario because the target's identity is not known and the facility or facilities cannot be described in advance. The situation may further be complicated as events condense, possibly into a crisis, where time is of the essence and available resources must be appropriately directed to employing surveillance to collect needed information instead of attempting to identify the nature and location of each of the facilities and places at which the electronic surveillance will be directed. Any requirement that the target be personally present at the computer or other facility only serves to complicate matters further, placing even more of a logistical strain on the timely collection of valuable information in a rapidly developing situation.

In summary, restricting FISA roving authority as suggested by the ACLU and other critics would roll back critical authority implemented under the PATRIOT Act to monitor terrorists and foreign agents with roving orders in instances where their identity is not known. This would effectively serve to reward terrorists for hiding their identities. Moreover, and quite disturbingly, terrorists are likely to *increase* anonymous infiltration in view of the heightened security measures undertaken by the government at customs and immigration check-points,

[111] Because e-mail accounts can be created with false information, it can be vital to an investigation to forthwith determine as much identifying information as possible when a person's true identity is not known.

thereby increasing the possibility that a target's identity will not be known in advance by the FBI when seeking a roving FISA order.

Conclusion

When the gathering storm threat of nuclear, biological and chemical weapons attack is considered against the backdrop of rapidly evolving digital personal communications technology, it would be negligent if not reckless to disallow the intelligence community the ability to conduct roving surveillance–which has been used under Title III for years–when appropriately needed in the context of counterterrorism. Faced with these escalating threats in this unconventional war, therefore, and after balancing the potential invasion of individual privacy interests as espoused by PATRIOT Act critics, defense attorneys and civil libertarians, it is clear that the benefits of Section 206 roving surveillance substantially outweigh the risks. Particularly in view of the technological advances and the sophistication of terrorists, roving FISA authority is not only a logical and lawful extension of preexisting authority under criminal law, it is a necessary one.

As Attorney General John Ashcroft aptly summed up the issue, "[s]ince 1986, we have effectively used roving wiretaps to track suspected drug dealers. Thanks to the Patriot Act, we can now use them to track the terrorist threat."[112]

[112] John Ashcroft, U.S. Attorney General, *Prepared Remarks (about the PATRIOT Act) of the Attorney General in Boise, Idaho* (August 25, 2003), available at: http://www.usdoj.gov/ag/speeches/2003/082503patriotactremarks.htm.