Electronic Surveillance and the Right To Be Secure

Timothy Casey[*]

In Katz v. United States*, the U.S. Supreme Court held that the Fourth Amendment limits the government's use of electronic surveillance. The* Katz *decision reoriented Fourth Amendment analysis in two important respects: the majority opinion of Justice Potter Stewart proclaimed that the Fourth Amendment "protects people, not places," and the concurring opinion of Justice John Marshall Harlan posited a "reasonable expectation of privacy" test to determine whether a given action of the state violated the Fourth Amendment. In the ensuing forty years, the* Katz *test has become the touchstone of Fourth Amendment analysis. The application of the* Katz *standard, however, has generated anomalous results, and the deficiencies of the* Katz *test are particularly apparent in the context of the government's use of new technologies to conduct electronic surveillance. Recent cases and decisions highlight both the advances in surveillance technologies and the inherent flaws in the reasonable expectation of privacy test. This Article suggests a return to the original language of the Fourth Amendment in order to preserve the right of the People to be secure.*

TABLE OF CONTENTS

[*] Associate Professor of Law, Case Western Reserve University School of Law. I thank Professors Lewis Katz, Raymond Shih Ray Ku, Anil Kalhan, Peter Friedman, and Lori Shellenberger for their insights, suggestions, and comments. Any errors or omissions remain my own.

INTRODUCTION

The U.S. Supreme Court's decision forty years ago in *Katz v. United States*[1] represented a paradigm shift in Fourth Amendment analysis.[2] Departing from a trespass-based theory of protection, *Katz* instructed that "the Amendment protects people, not places,"[3] and provided courts with the now-familiar "reasonable expectation of privacy" metric to determine whether a governmental action triggers the protection of the Fourth Amendment.[4] The legacy of *Katz*, however, has been mixed.[5]

Recent controversies involving the government's expanded use of technological capabilities highlight the difficulties modern courts face when navigating issues in the field of electronic surveillance. In December of 2005, President George W. Bush announced that the government had secretly launched a massive electronic surveillance and communications interception program.[6] Although the President asserted that the Terrorist Surveillance Program ("TSP") was

[1] 389 U.S. 347 (1967).

[2] Regarding paradigm shifts, see generally THOMAS S. KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (1962) (describing process of scientific discovery and progress). Kuhn postulated that science advances in spurts, which he termed paradigm shifts. Paradigm shifts occur when sufficient evidence accumulates to refute the presumption that a given theory is correct. *Id.* at 18-19, 23-24.

[3] *Katz*, 389 U.S. at 353 ("[T]he 'trespass' doctrine . . . can no longer be regarded as controlling.").

[4] *Id.* at 361 (Harlan, J., concurring).

[5] Numerous commentators have described the amorphous nature of Fourth Amendment jurisprudence. *See, e.g.*, Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 385-86 (1974) (describing all or nothing approach of Fourth Amendment); *see also* Ronald Allen & Ross Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1149 (1998) ("The Supreme Court cases construing the Fourth Amendment are a mess that lacks coherence and predictability, and fails to communicate the contours of the field."); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 759-61 (1994); Sherry Colb, *Innocence, Privacy and Targeting in Fourth Amendment Jurisprudence*, 96 COLUM. L. REV. 1456, 1512 (1996) (commenting specifically on distorting effect of application of exclusionary rule in Fourth Amendment contexts); Raymond Shih Ray Ku, *Modern Studies in Privacy Law: Searching for the Meaning of Fourth Amendment Privacy After* Kyllo v. United States*: The Founder's Privacy: The Fourth Amendment and the Power of Electronic Surveillance*, 86 MINN. L. REV. 1325 (2002) (arguing Fourth Amendment should properly be conceived as mechanism for separating powers of government).

[6] President George W. Bush, White House Press Conference (Dec. 19, 2005), *available at* http://www.whitehouse.gov//news/releases/2005/12/20051219-2.html.

"consistent with U.S. law and the Constitution,"[7] a group of lawyers and journalists disagreed and, in *ACLU v. NSA*, averred that the government illegally intercepted their communications under the auspices of the TSP.[8] Simultaneously, in *Hepting v. AT&T*, a class of citizen plaintiffs alleged that one of the world's largest telecommunications corporations unlawfully allowed the government to intercept communications and Internet information carried across its network.[9] Similar lawsuits filed in several other jurisdictions were consolidated and transferred to Judge Vaughn Walker in the Northern District of California, where *Hepting* was pending.[10] In these cases (collectively, the "NSA Cases"), the government declined to address the substantive claims and instead asserted the "state secrets privilege," arguing that the cases should be dismissed in the interest of national security.[11]

The disclosure of a secret and far-reaching government surveillance program coincided with a growing discomfort within the federal judiciary regarding the government's use of a surveillance device known as a pen register.[12] In August of 2005, in a decision of first impression, federal Magistrate Judge James Orenstein of the Eastern District of New York denied, in part, the government's ex parte application for a pen register on a cell phone.[13] The core issue before

[7] *Id.*

[8] ACLU v. NSA, 438 F. Supp. 2d 754, 758 (E.D. Mich. 2006), *rev'd*, 493 F.3d 644, 688 (6th Cir. 2007). Plaintiffs alleged violation of the First and Fourth Amendments as well as numerous statutory violations.

[9] Hepting v. AT&T, 439 F. Supp. 2d 974, 978-80 (N.D. Cal. 2006).

[10] *In re* NSA Telecomms. Records Litig., 474 F. Supp. 2d 1355, 1356 (J.P.M.L. 2007) (ordering transfer of actions pursuant to Multi-District Litigation Rule 7.4 to Judge Walker in Northern District of California), *motion to remand to state court denied*, NSA, 483 F. Supp. 2d 934, 947 (N.D. Cal. 2007); *In re* NSA Telecomms. Records Litig., 444 F. Supp. 2d 1332, 1335 (J.P.M.L. 2006); *see also* Al-Haramain Islamic Found., Inc. v. Bush, 451 F. Supp. 2d 1215, 1217 (D. Or. 2006).

[11] *ACLU*, 438 F. Supp. 2d at 758; *Hepting*, 439 F. Supp. 2d at 979-80. The Sixth Circuit denied standing to the plaintiffs in *ACLU v. NSA*, 493 F.3d 644, 687-88 (6th Cir. 2007). The plaintiffs have appealed to the U.S. Supreme Court, but a docket number has not been assigned. *Hepting v. AT&T* is pending before the Ninth Circuit Court of Appeals, and was recently severed from *Al-Haramain Islamic Found., Inc. v. Bush*. Hepting v. AT&T, Nos. 06-17132, 06-17137, 2007 U.S. App. LEXIS 26569 (9th Cir. Nov. 16, 2007).

[12] A "pen register" is a "device or process which records or decodes routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . . ." 18 U.S.C. § 3127(3) (2000 & Supp. V 2005).

[13] *In re* Application of the United States for an Order (1) Authorizing the Use of a

Magistrate Judge Orenstein was whether the government could use new technology to convert a pen register into a personal tracking device without a warrant. The government's application requested cell site location information at the time of the call and during the call, information that would allow government agents to verify the identity and location of the user of the subject cell phone.[14] Magistrate Judge Orenstein denied the request for location information on the grounds that neither existing statutes nor the Constitution authorized the government to access the personal tracking information without a warrant.[15] The publication of his decision sparked a controversy within the judiciary, prompting at least fifteen contradictory decisions (collectively, the "Pen Register Decisions").[16]

At the heart of both the NSA Cases and the Pen Register Decisions lies the struggle to reconcile the use of expanding technological

Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. & Cell Site Info., 384 F. Supp. 2d 562 (E.D.N.Y. 2005) [hereinafter *Orenstein I*], *motion to reconsider denied*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) [hereinafter *Orenstein II*].

[14] *Orenstein I*, 384 F. Supp. 2d at 563-64; *Orenstein II*, 396 F. Supp. 2d at 294-95.

[15] *Orenstein I*, 384 F. Supp. 2d at 564; *Orenstein II*, 396 F. Supp. 2d at 300.

[16] *In re* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448 (S.D.N.Y. 2006) [hereinafter *Kaplan*] (granting cell site location information); *In re* Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info., No. 06-Misc-004, 2006 U.S. Dist. LEXIS 73324 (E.D. Wis. Oct. 6, 2006) [hereinafter *Adelman*] (denying cell site information); *In re* Application for an Order Authorizing the Installation & Use of a Pen Register & Directing the Disclosure of Telecomm. Records for the Cellular Phone Assigned to the No. [Sealed], 439 F. Supp. 2d 456 (D. Md. 2006) (denying cell site location information); *In re* Application of the United States for Prospective Cell Site Location Info. on a Certain Cellular Tel., No. 06-Crim-Misc-01, 2006 U.S. Dist. LEXIS 11747 (S.D.N.Y. Mar. 2, 2006) [hereinafter *Peck*] (denying cell site location information, and implying that government was avoiding further litigation of issue); *In re* Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace for Mobile Identification No. (585) 111-1111 & the Disclosure of Subscriber & Activity Info. Under 18 U.S.C. § 2703, 415 F. Supp. 2d 211 (W.D.N.Y 2006) [hereinafter *Feldman*] (denying cell site location information); *In re* Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; & (2) Authorizing the Release of Subscriber Info. & Cell Site Info., 411 F. Supp. 2d 678 (W.D. La. 2006) (granting cell site location as to single tower during calls, but denying location information when no call is in progress, denying triangulation information and denying GPS information); *In re* Application of the United States for an Order for Disclosure of Telecomm. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (granting cell site location information) [hereinafter *Gorenstein*]; *In re* Application for a Pen Register & Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 2005) (denying government's request for cell site tracking) [hereinafter *Smith*].

capabilities with a labyrinth of statutes and a problematic standard of constitutional review. The NSA Cases alert us to the very real possibility that the executive branch has the capacity to monitor every transaction and communication of any individual without the check of judicial review. The Pen Register Decisions involve requests for judicial orders permitting real time tracking of individuals by the government based on a mere certification that the information is relevant to an investigation. Both sets of cases provide an impetus to reexamine the increasingly complicated intersection of law, advancing technology, and our conceptions of personal and national security.

The increased capacity for electronic surveillance and the need to employ new technologies require a critical reassessment of the existing legal structure. In essence, it is time for another paradigm shift.[17] We must abandon *Katz*'s reasonable expectation of privacy and adopt language that accurately reflects the significance of the interests protected by the Fourth Amendment. The interests that courts since *Katz* have described in terms of a reasonable expectation of privacy should be expressed in terms of personal security and the right to be secure. At first blush it may appear that replacing the reasonable expectation of privacy with the right to be secure is merely a game of semantics, but the use of specific language is important, and reclaiming the language of security will provide greater clarity and guidance in our analysis of Fourth Amendment issues.[18]

This Article proceeds in three parts. Part I briefly outlines the framework of laws regulating electronic surveillance, first examining constitutional rulings and then reviewing the major pieces of legislation in the field. Part II describes the technological advances since *Katz* was decided, with particular attention to the development of the Internet and cell phones. Part II examines, through the NSA Cases and the Pen Register Decisions, the difficulties in applying the reasonable expectation of privacy standard in our current legal and technological environment. Part III suggests that we should respond to modern challenges by moving beyond the *Katz* standard and reclaiming the original language and meaning of the Constitution.

---

[17] *See* KUHN, *supra* note 2, at 19, 23-24; *see also* Peter Swire, Katz *is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 910 (2004).

[18] "Words, however, have connotations that can color, sharpen or diffuse meaning: this can help those drawing lines in the sand find some common ground . . . ." William Safire, *On Language: Benchmark and Timetable*, N.Y. TIMES, May 27, 2007, § b (Magazine), at 14.

I. LEGAL FRAMEWORK OF ELECTRONIC SURVEILLANCE[19]

Historically, the Fourth Amendment has protected the lives and property of the People by ensuring "a right to be secure" against unreasonable government intrusions.[20] The Amendment was born of a reaction to the historical abuses of English general writs and writs of assistance. Under the authority of these writs, law enforcement agents could obtain a warrant of general authority to search premises at any time and seize any property, and they could enlist local citizens to assist in the project. In *Entick v. Carrington*,[21] Lord Camden reviewed the legality of the English writs and ruled that a warrant to search must be judged on its legal merits, not merely on whether it was issued by a government agent.[22] American orators delivered great speeches directed against the evils of the writs and the exercise of unbridled discretion at the hands of government agents. In a speech at the Superior Court in Boston in 1761, James Otis famously deemed the writ of assistance as "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law . . . ." [23] John Adams reported Otis's speech and noted that with this oration, "American independence was born."[24]

The Framers recognized the importance of the right of the People to be secure and free from discretionary and disruptive governmental intrusion into their lives. The Fourth Amendment established a right to be secure against unreasonable searches and seizures by the government. In Fourth Amendment jurisprudence, the threshold issue is whether a specific action or intrusion by the government constitutes a "search" within the meaning of the Amendment. [25] In

---

[19] Readers familiar with the substantive law may want to skip to Part III.

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

[21] (1765) 95 Eng. Rep. 807 (K.B.), *available at* http://www.bailii.org/ew/cases/EWHC/KB/1765/J98.rtf.

[22] *Id.*

[23] James Otis, Speech at the Superior Court in Boston: In Opposition to the Writs of Assistance (Feb., 1761), *in* [8 America – 1] THE WORLD'S FAMOUS ORATIONS 27-36 (William Jennings Bryan, ed., Funk & Wagnalls Co. 1906), *available at* http://www.bartleby.com/268/8/9.html.

[24] *Id.* at 27 n.1; *see also* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) (referencing Otis's speech and Lord Camden's decision).

[25] A government intrusion into the "persons, houses, papers and effects" will be deemed a "search" or "seizure," and any such search or seizure by the government

any action deemed to be a search, the government must comply with the requirements of the Amendment: (1) obtain a warrant from a neutral magistrate; (2) based upon probable cause; (3) supported by sworn affidavits; (4) particularly describing the places to be searched and the things to be seized.[26] Any action not deemed a search, however, falls outside the ambit of the Amendment and leaves government agents restricted only by their own discretion.[27] One noted commentator, Professor Anthony Amsterdam, described Fourth Amendment jurisprudence as an "all-or-nothing approach."[28]

A. The Fourth Amendment and Electronic Surveillance

Technological advances frequently have challenged the limits of Fourth Amendment jurisprudence, resulting in gaps of uncertainty in the interface between the People and the government.[29] Legislation regulating electronic surveillance has filled these gaps. Frequently the legislation and the jurisprudence follow a tit-for-tat pattern, with the legislature responding to an unsavory decision with new laws, only to have the courts interpret the new legislation in light of technological advances.[30]

Professor Amsterdam's all-or-nothing approach aptly describes many areas of Fourth Amendment jurisprudence, but specific statutory regulations have created more levels of gradation in the area

requires a warrant based on probable cause and supported by an affirmation "particularly describ[ing] the place to be searched or the person or thing to be seized." U.S. CONST. amend IV.

[26] *Id.*

[27] Amsterdam, *supra* note 5, at 388.

> ("[W]herever [the Fourth Amendment] restricts police activities at all, it subjects them to the same extensive restrictions that it imposes upon physical entries into dwellings. To label any police activity a "search" or "seizure" within the ambit of the amendment is to impose those restrictions upon it. On the other hand, if it is not labeled a "search" or "seizure," it is subject to no significant restrictions of any kind. It is only "searches" or "seizures" that the fourth amendment requires to be reasonable; police activities of any other sort may be as unreasonable as the police please to make them.").

[28] *Id.*

[29] *See infra* Part III.A; *infra* notes 153-72 and accompanying text. As described below, no other area of Fourth Amendment jurisprudence has been so greatly supplemented with additional legislation.

[30] *See infra* notes 102-52 and accompanying text; *see also* DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 262-63 (2d ed. 2006); Swire, *supra* note 17, at 917.

of electronic surveillance than in other search and seizure contexts.[31] Thus even where a specific type of intrusion is not considered a search, and therefore not subject to constitutional limitation, the statutory regime requires that government agents abide by specific procedures, which often include judicial review. For example, if government agents wanted to use a pen register on a landline telephone, they would not be limited by the Constitution because the Supreme Court held that the use of a pen register does not implicate the Fourth Amendment.[32] However, the Pen Register Act requires that the government agents obtain a judicial order based on a showing far below probable cause before they can legally employ the pen register.[33]

Electronic surveillance by the government differs from other types of governmental intrusions because typically there is no seizure of tangible property, no search of a defined structure or place, and if properly executed, no knowledge of the government's action by the target of the search. Early cases recognized but quickly dismissed the distinction between an overt search and a search by stealth. In *Gouled v. United States*, Justice John Clarke found no distinction between intrusions by force, coercion, or stealth: all violated the privacy and security interests of the citizen and implicated the Fourth Amendment equally. [34]

Although Justice Clarke spoke of privacy and security as inseparable facets of the interest protected by the Fourth Amendment, later cases did not maintain the language of security.[35] In *Olmstead v. United States*, the Court held that the connection of a wiretapping device to the telephone lines did not violate the Fourth Amendment because the intrusion was accomplished "without trespass on any property of the defendants."[36] Likewise, in *Goldman v. United States*, the Court found no Fourth Amendment violation where a listening device was placed on an outer wall because there was no physical encroachment on the

[31] RONALD ALLEN, RICHARD KUHNS & WILLIAM STUNTZ, CONSTITUTIONAL CRIMINAL PROCEDURE: AN EXAMINATION OF THE FOURTH, FIFTH, AND SIXTH AMENDMENTS AND RELATED AREAS 541-43 (2000).

[32] *See infra* notes 81-89 and accompanying text (discussing pen registers in *Smith v. Maryland*).

[33] *See infra* notes 133-35 and accompanying text (discussing Pen Register Act).

[34] "[I]t is impossible to successfully contend that a [search and seizure] would be a reasonable one if only admission were obtained by stealth instead of by force or coercion. The security and privacy of the home or office and of the papers of the owner would be as much invaded and the search and seizure would be as much against his will in the one case as in the other . . . ." 255 U.S. 305-06 (1921).

[35] *Id.*

[36] 277 U.S. 438, 457 (1928).

defendant's property.[37] In *Silverman v. United States*, the Court held that a Fourth Amendment violation occurred when agents inserted a "spike mike" into a party wall.[38] Thus, where agents placed an eavesdropping device within the walls of the target's building — crossing the threshold — the action was deemed a search, but when the device was placed just outside the building, it was not a search.[39] The conception of the Fourth Amendment as an extension of one's property rights continued until 1967, when the Court decided *Berger v. New York* and *Katz v. United States*.

1. 1967: *Berger* and *Katz*

In a discussion of the constitutional aspects of electronic surveillance, 1967 presents a logical starting point. Of course, there are many important decisions both before and after 1967, but the decisions in *Berger v. New York* and *Katz v. United States* stand starkly apart because they dealt both factually and legally with the use of new technologies. *Berger* and *Katz*, however, cannot be read without reference to *Olmstead v. United States*,[40] where the Court ruled, over a notorious dissent by Justice Louis Brandeis,[41] that wiretapping by the government did not implicate the Fourth Amendment. Nor can *Berger* and *Katz* be properly understood without reference to section 605 of the Communications Act of 1934, the legislative response to *Olmstead* that banned all "interception" of "wire communications."[42]

Berger highlighted the concerns over new wiretapping technologies and the increased use of electronic surveillance by law enforcement. In striking down a New York statute that permitted law enforcement to eavesdrop electronically, the Court focused on the particularity requirement of the Fourth Amendment. The statute at issue in *Berger* permitted a state judge to issue an order permitting electronic surveillance, including surreptitious recording of the content of conversations, upon a showing of reasonable cause to believe evidence

[37] 316 U.S. 129, 134 (1942). In fact, government agents had previously broken into the defendant's house to install a listening device, but because the device malfunctioned and the government did not seek to introduce evidence stemming from the break-in the Court discounted the earlier trespass as inconsequential to the Fourth Amendment analysis. *Id.* at 134-35.

[38] 365 U.S. 505, 512 (1961).

[39] *See id*; *Goldman*, 316 U.S. at 134-36; *Olmstead*, 277 U.S. at 457, 464, 466.

[40] 277 U.S. 438.

[41] *Id.* at 471 (Brandeis, J., dissenting).

[42] Communications Act of 1934, ch. 652, 48 Stat. 1064, 1103 (codified as amended at 47 U.S.C. § 605 (2000)).

of a crime would be discovered. Notably, the *Berger* Court analyzed the Fourth Amendment issue by analogy to trespass, as demonstrated by its reference to an amorphous "constitutionally protected area."[43] The substance of the decision, however, represents a break from the trespassory analysis mandated by *Olmstead*, a point noted by Justice William Douglas in the opening line of his concurring opinion.[44]

Katz signified a paradigm shift in Fourth Amendment jurisprudence[45] — a shift away from the traditional "property trespass" theory of Fourth Amendment protection.[46] Before *Katz*, constitutional protection was afforded only to physical places.[47] By noting that the "amendment protects people, not places,"[48] the *Katz* Court instructed that future intersections of government and citizen interests would be regulated by a new barometer — the "reasonable expectation of privacy."[49]

Factually, the *Katz* case involved criminal charges of transmitting wagering information across state lines. The government sought to introduce evidence of Charles Katz's conversations obtained from an electronic surveillance device placed on a public phone booth that

[43] Berger v. New York, 388 U.S. 41, 44 (1967) ("We have concluded that the language of New York's statute is too broad in its sweep resulting in a *trespassory intrusion* into a constitutionally protected area and is, therefore, violative of the Fourth and Fourteenth Amendments." (emphasis added)).

[44] *Id.* at 64 (Douglas, J., concurring) ("I join the opinion of the Court because at long last it overrules *sub silentio Olmstead v. United States*, 277 U.S. 438, and its offspring and brings wiretapping and other electronic eavesdropping fully within the purview of the Fourth Amendment.").

[45] At least one commentator has suggested that we are now at the point of another paradigm shift, and that the era of *Katz* has ended. Swire, *supra* note 17, at 910. *See generally* KUHN, *supra* note 2, at 18-19, 23-24.

[46] Goldman v. United States, 316 U.S. 129, 134-36 (1942); *Olmstead*, 277 U.S. at 457, 464, 466. *But see Berger*, 388 U.S. at 64 (Douglas, J., concurring) (noting Court's decision in *Berger* overruled *Olmstead* sub silentio).

[47] Katz v. United States, 389 U.S. 341, 361 (1967) (Harlan, J., concurring). *Compare Goldman*, 316 U.S. at 134-36, *and Olmstead*, 277 U.S. at 464-66, *with* Silverman v. United States, 365 U.S. 505, 511 (1961). *Katz* explicitly rejected the trespass doctrine of *Olmstead*: "We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling." *Katz*, 389 U.S. at 353.

[48] *Katz*, 389 U.S. at 351 (majority opinion).

[49] *Id.* at 361 (Harlan, J., concurring). I do not mean to imply that the Court consciously decided to create a new standard. Indeed, the "reasonable expectation of privacy" language derives from Justice Harlan's concurring opinion. However, regardless of the actual intent of the authors, the "reasonable expectation of privacy" has endured and has assumed a dominant position in Fourth Amendment analysis in the 40 years since *Katz*.

Katz used to place bets. The district court denied Katz's suppression motion and the Ninth Circuit affirmed the district court's determination.[50]

Reversing the Ninth Circuit, the Supreme Court provided language that continues to govern Fourth Amendment analysis.[51] Justice Stewart's majority opinion famously held that "the Fourth Amendment protects people, not places."[52] Significantly, the Court's analysis focused on privacy interests and whether Katz was justified in his reliance on the secrecy of his conversations: "The government's activities . . . violated the privacy upon which he justifiably relied . . . ."[53] The effect of the transition from protection of places to protection of people held particular significance for electronic surveillance because the Fourth Amendment could thereafter apply to intangible interests, such as Katz's conversation.

In his concurring opinion, Justice Harlan penned the bifurcated standard of reasonableness that has come to control our current analysis of whether government activities illegally intrude upon privacy interests: "[A] person has a constitutionally protected reasonable expectation of privacy" governed by a two-fold requirement 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."[54] Justice Harlan's standard provided future courts with a test to determine whether the government intrusion — whether upon a tangible property interest or upon an intangible interest — would be subject to regulation by the Fourth Amendment.

In his dissent, Justice Hugo Black focused on the use of particular language, specifically objecting to the inclusion of the word "privacy."[55] He preferred a strict construction of the Amendment, which would limit searches to "persons, houses, papers and effects."[56] In Justice Black's textual view, the Constitution did not contain a right to privacy, and the concurring Justices were using the Fourth

[50] Katz v. United States, 369 F.2d 130, 135 (9th Cir. 1966).

[51] *Katz*, 389 U.S. at 360-62 (Harlan, J., concurring).

[52] *Id.* at 350-54 (majority opinion).

[53] *Id.*

[54] *Id.* at 360-62 (Harlan, J., concurring) (internal quotation marks omitted). Later decisions have whittled the bifurcated standard into a unitary issue of the objective reasonableness of the expectation of "privacy."

[55] *Id.* at 364 (Black, J., dissenting).

[56] *Id.*

Amendment as a "vehicle" for overturning laws that offended "the Court's broadest conception of privacy."[57]

Thus, the *Katz* Court accomplished two significant maneuvers. First, Justice Stewart's majority opinion shifted the focus of the Fourth Amendment from places to people, thereby clearing the way for the application of the Amendment to intangible interests, including the fruits of electronic surveillance. Second, the language from Justice Harlan's concurrence provided a resilient test. Since *Katz*, the controlling question in Fourth Amendment analysis is whether the action of the government agents violates a reasonable expectation of privacy in the area searched or the thing seized.[58] The *Katz* standard remains the analytical touchstone for determining whether electronic surveillance by the government constitutes a mere observation or a constitutionally protected search.[59]

2. Executive v. Judiciary: *United States v. United States District Court*

A few years after *Berger* and *Katz*, the issue of electronic surveillance remained at the center of national attention. On June 17, 1972, five men were arrested during an attempted burglary of the offices of the Democratic Party at the Watergate Hotel in Washington, D.C.[60] Two days later, the Supreme Court decided *United States v. United States District Court* ("*Keith*").[61] Both controversies pitted the branches of government against one another.

In the *Keith* case, the power of the President to ensure national security clashed with the duty of the judiciary to faithfully enforce the Constitution.[62] Procedurally, the case arose during the prosecution of

---

[57] *Id.* Harlan's concurrence and Black's dissent characterize the issue in terms of a "privacy" interest, which can be traced directly to Justice Brandeis's dissent in the *Olmstead* decision.

[58] Kyllo v. United States, 533 U.S. 27, 33 (2001) ("[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy society recognizes as reasonable."); *see also* Oliver v. United States, 466 U.S. 170, 177 (1984) ("Since [*Katz*], the touchstone of Amendment analysis has been whether a person has a 'constitutionally protected reasonable expectation of privacy.'" (citations omitted)).

[59] *See* Illinois v. Caballes, 543 U.S. 405, 408-09 (2005).

[60] I do not mean to imply any connection between the arrest at the Watergate Hotel and the Court's decision, other than mere serendipity. Indeed, the full extent of the Watergate Conspiracy was not known until the next year after the trial of the apprehended men.

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

[62] *Id.* at 321.

defendants charged with conspiring to bomb the office of the Central Intelligence Agency in Ann Arbor, Michigan.[63] The executive branch, through the Attorney General, had authorized domestic wiretaps without judicial approval. The defendants moved for disclosure of any statements obtained through the use of electronic surveillance.[64] The executive branch argued that the President had inherent constitutional authority to conduct wiretaps where reasonably necessary to prosecute, investigate, or prevent threats to national security.[65] The government asserted that the surveillance "was lawful, though conducted without prior judicial approval, as a reasonable exercise of the President's power to protect the national security."[66]

Rejecting the arguments of the executive branch, the District Court for the Eastern District of Michigan found that the surveillance violated the Fourth Amendment, and ordered the government to make the information available to the defendants.[67] Rather than comply with the district court's order, the government filed a writ of mandamus to the Sixth Circuit Court of Appeals, challenging the validity of the district court's order. When the Sixth Circuit agreed with the district court, the government appealed to the Supreme Court.[68]

Initially, the majority opinion of Justice Lewis Powell focused on an issue of statutory interpretation[69] — whether recently enacted

[63] *Id.* at 299.

[64] *Id.*

[65] *Id.* at 302.

[66] *Id.* at 301.

[67] United States v. Sinclair, 321 F. Supp. 1074, 1080 (E.D. Mich. 1971). Recently, the Eastern District of Michigan again rejected similar arguments made by the executive branch in *ACLU v. NSA*. *See infra* notes 214-19 and accompanying text.

[68] United States v. U.S. Dist. Court (*Keith*), 444 F.2d 651, 669 (6th Cir. 1971), *aff'd*, 407 U.S. 297 (1972).

[69] Specifically, the language at issue derived from 18 U.S.C. § 2511(3) (2000):

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

legislation, the Omnibus Crime Control and Safe Streets Act of 1968, conferred on the President the additional power to conduct domestic electronic surveillance where such surveillance was related to issues of national security.[70] After confirming that the legislation neither conferred additional power on the President nor limited constitutionally vested authority of the President, the Court turned to the more delicate issue of whether the President was authorized under Article II of the Constitution to conduct domestic wiretapping without a court order.[71] The Court refined the issue to the circumstances of the case, which involved an asserted interest in national security, but no foreign power or interests.[72]

The Court noted its role in balancing competing interests:

> [O]ur task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression . . . . [Specifically,] whether the needs of citizens for privacy and free expression may not be better protected by requiring a warrant before such surveillance . . . [and] whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it.[73]

In holding that the warrant clause of the Fourth Amendment was not "dead language,"[74] the Court affirmed the district court's order. Justice Powell's opinion concluded by suggesting (or predicting) that Congress might appoint a "specially designated court" to entertain warrant applications in particularly sensitive cases.[75] In concurrence, Justice Douglas presciently restated the dangers of "unchecked

> evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.

[70] *Keith*, 407 U.S. at 302 ("Congress recognized the President's authority to conduct [national security] surveillances without prior judicial approval.")

[71] *Id.* at 310.

[72] *Id.* ("Nor is there any doubt as to the necessity of obtaining a warrant in the surveillance of crimes unrelated to the national security interest.")

[73] *Id.* at 315.

[74] *Id.*

[75] Justice Powell's language predicted the action of Congress in enacting the Foreign Intelligence Surveillance Act. *Id.* at 323.

discretion" by the executive and the intelligence "machine."[76] He also noted the lack of a sufficient remedy in cases of unjustified or unreasonable intrusions because the victim of the transgression would have no idea that her rights had been violated.[77]

The *Keith* case reaffirmed the notion that the Fourth Amendment is fundamentally concerned with the separation of powers — specifically, the limitation of the power of the executive branch.[78] The case also demonstrated the tit-for-tat pattern by predicting congressional action in the form of the Foreign Intelligence Surveillance Act.[79] Coincidentally, the *Keith* case arose in the Eastern District of Michigan, the same jurisdiction as one of the NSA Cases, *ACLU v. NSA*.[80]

3. Pen Registers: *Smith v. Maryland*

In *Smith v. Maryland*, the Court confronted the issue of whether a person had a reasonable expectation of privacy in telephone numbers he had dialed from within his home.[81] *Smith* involved electronic surveillance in the form of a pen register, which, at the time of the Court's decision, was "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released."[82] Significantly, the device did not "overhear" oral communications, and was not capable of determining whether or not the call was completed.[83] The pen register device was attached, without a warrant, to the phone line of the suspect in order to determine the origin of calls made to a robbery victim.[84]

---

[76] *Id.* at 325 (Douglas, J., concurring).

[77] *Id.*; *see also* Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 391-97 (1971) (permitting private cause of action for unlawful search incident to arrest in violation of Fourth Amendment).

[78] *See* Ku, *supra* note 5, at 1337 ("[A] primary goal of the Fourth Amendment is the same as that of the entire Constitution — to define and limit governmental power.").

[79] *See infra* Part II.B.3.

[80] *See infra* Part III.C.

[81] 442 U.S. 735 (1979).

[82] *Id.* at 736 n.1. I note the distinction between the 1971 device examined by the Court in *Smith v. Maryland* because it differs so dramatically from the technology in current pen registers. *See infra* notes 153-72 and accompanying text.

[83] *Smith*, 442 U.S. at 736 n.1.

[84] *Id.* at 736-37. The phone company installed the pen register at its central offices at the request of the police. *Id.* at 740 n.4. Notably, the pen register device was placed on the phone of the suspect, rather than on the phone of the recipient of the

The Court, in an opinion by Justice Blackmun, held that the installation and monitoring of the pen register device did not constitute an intrusion into an area protected by a reasonable expectation of privacy.[85] The *Smith* Court adopted the two-prong analysis suggested by Justice Harlan in *Katz*: whether the petitioner entertained a subjective expectation of privacy in the area, and if so, whether the expectation of privacy was one that society would be willing to accept as objectively reasonable.[86] In its analysis, the Court slid past the first prong and focused on the illegitimate nature of an expectation of privacy in numbers dialed from one's home: "We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.'"[87]

The *Smith* case is significant for several reasons. The Court's description of a 1971 pen register highlights the dramatic change in the capability of a 2007 pen register. The Court's decision explicitly relied upon the limited capabilities of the pen register and the exposure of the dialing information to the telephone company.[88] From a jurisprudential perspective, *Smith* demonstrated the Court's tendency to equate the privacy interest indentified in *Katz* with secrecy, such that exposure of the information to any third party destroyed the reasonable expectation of privacy.[89]

4. Tracking Devices: *United States v. Knotts* and *United States v. Karo*

In 1983 and 1984, the Supreme Court granted certiorari in two cases involving tracking devices. In *United States v. Knotts*, government agents placed a tracking device in a drum of chemicals

calls. If law enforcement had used a "trap and trace" device, they would have obtained the same information — that a call was placed from the suspect's phone to the recipient's phone — without raising the issue of a nonconsensual intrusion.

[85] *But see* Sherry Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hint of a Remedy*, 55 STAN. L. REV. 119, 120 (2002). Professor Colb offers a poignant criticism of the dissonance in the Court's reasoning that exposure to one is equal to exposure to the world. *Id.* at 153-61.

[86] *Smith*, 442 U.S. at 736.

[87] *Id.* at 745-46.

[88] *Id.* at 742.

[89] *See* Miller v. United States, 425 U.S. 435, 442-44 (1976) (holding persons have no reasonable expectation of privacy in banking records); *see also* Colb, *supra* note 85, at 122-26, 153-61 (discussing Court's assumption that acceptance of risk of exposure is equal to exposure and Court's flawed logic in equating exposure to one as exposure to world).

that was delivered to the defendants, enabling the agents to track the movements of the chemicals and the location of the defendants.[90] Analogizing the public highway to open fields, the Court held that the placement of the device and the monitoring of the defendant's location through the device did not implicate the Fourth Amendment because the tracking occurred on public roads, where the agents could have visibly observed the defendants.[91] The tracking device in *Knotts* merely enhanced the sensory capabilities of the agents.

Just a year later, the Court revisited the issue in *United States v. Karo*.[92] In *Karo*, agents again put a tracking device in a container placed with the defendants; however, the agents continued to monitor the tracking device after it was transported into a private residence. The Court declined to extend the *Knotts* "public highway" analysis to all locations: when the agents obtained information from the interior of the residence, the action was deemed a search, triggering Fourth Amendment protections. Thus, tracking devices were permissible and did not implicate the Fourth Amendment, so long as the tracking occurred on public roads.[93]

These cases demonstrate the tenuous nature of the Court's position with respect to electronic surveillance. In *Knotts* and *Karo*, a single factor distinguished the outcome in two factually similar cases — whether the device transmitted electronic signals from inside the home. Thus even with the reasonable expectation of privacy standard, the area protected by the Fourth Amendment was essentially defined by the threshold to the home.

---

[90] 460 U.S. 276, 278 (1983).

[91] *Id.* at 281-82. "[N]o such expectation of privacy extended to the visual observation of Petschen's automobile arriving on his premises after leaving a public highway, nor to movements of objects such as the drum of chloroform outside the cabin in the "open fields." *Id.* at 282. In *Hester v. United States*, 265 U.S. 57, 59 (1924), the Court held that the Fourth Amendment's list of protected areas did not include open fields. Later, in *Oliver v. United States*, 466 U.S. 170, 178-81 (1984), the Court used the open fields language of *Hester* to explain why the defendant in *Oliver* did not have a reasonable expectation of privacy in the area surrounding his home.

[92] 468 U.S. 705, 721 (1984).

[93] *Id.* at 721; *Knotts*, 460 U.S. at 281-82; United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006) (permitting evidence obtained from tracking device, but suppressing evidence obtained from device while in defendant's home); *see* United States v. McIver, 186 F.3d 1119, 1127 (9th Cir. 1999) (finding no warrant necessary for installation of GPS tracking device on vehicle under *Knotts* rationale).

5. Home Surveillance: *United States v. Kyllo*

The Court has consistently held that the Fourth Amendment protects the interior of the home from warrantless governmental intrusion.[94] In *Kyllo v. United States*,[95] the Court examined the use of an investigative tool that produced thermal images from the interior of the home. In finding that the actions of the agents violated the Fourth Amendment, *Kyllo* reaffirmed the Court's reliance on property principles in determining the application of the Fourth Amendment, and reiterated the message from earlier cases, such as *Karo*, that the home is indeed protected by the Fourth Amendment. Significantly, *Kyllo* also provided some insight into how the Court might handle future cases involving technological advances. Justice Antonin Scalia, in the majority opinion, drew a "firm but also bright" line marking the limit of Fourth Amendment application where government agents acquired "by sense-enhancing technology, any information regarding the home's interior that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' . . . at least where (as here) the technology in question is not in general public use."[96] Justice John Paul Stevens, in dissent, sharply disagreed with Justice Scalia, in particular, on the issue of the general public use exception: "Putting aside its lack of clarity, this criterion is somewhat perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."[97]

The *Kyllo* decision demonstrates the difficulty in applying the *Katz* standard with its link to the normative question of whether the expectation of privacy was reasonable. Justice Scalia's rationale held that technologies in general public use would not be subject to Fourth Amendment regulation because there is a normative expectation that the technology will be used, and thus there can be no reasonable expectation of privacy in the information that the device reveals.[98]

---

[94] In a series of cases, the Court found that the Fourth Amendment did not prohibit government agents from monitoring property through aerial surveillance. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 452 (1989); California v. Ciraolo, 476 U.S. 207, 213 (1986).

[95] 533 U.S. 27, 33 (2001).

[96] *Id.* at 34, 40.

[97] *Id.* at 47 (Stevens, J., dissenting). Much of the disagreement between Justice Scalia and Justice Stevens revolves around the technological capability of the device in question. *Compare id.* at 33-34 (majority opinion), *with id.* at 42-50 (Stevens, J., dissenting).

[98] *Id.* at 34 (majority opinion); *id.* at 41-44, 46-48 (Stevens, J., dissenting); *see also*

Justice Stevens noted that because the normative aspect of the reasonable expectation of privacy standard changes in tandem with evolving technologies in the area of electronic surveillance, the level of Fourth Amendment protection decreases as a technology becomes more common. In sum, *Kyllo* makes clear that the *Katz* standard muddies the question of what is subject to Fourth Amendment regulation and guarantees that levels of constitutional protection will vary with technological innovation and inevitably decrease depending on rates of popular adoption of new technologies.

6. Summary of Constitutional Framework

The electronic surveillance cases were difficult to fit into the traditional property-trespass rubric of the Fourth Amendment. While the change from a property-trespass theory to a privacy-based theory permitted courts to apply the Fourth Amendment's protection to intangible interests, it also led to the equating of privacy with secrecy. *Katz* signified a shift away from the property-trespass theory of Fourth Amendment analysis by finding a constitutionally protected interest separate from any place and distinct from tangible property. Later cases, however, have tended to revert to a property-trespass-based analysis. For example, the tracking devices in *Karo* and *Knotts* did not implicate the Fourth Amendment until there was an intrusion into the home.[99] Likewise, surveillance directed at the private yard was treated differently from surveillance directed to the inside of the home.[100] Several commentators have criticized the trend to equate the reasonable expectation of privacy with secrecy, such that once the information has been released, the Fourth Amendment does not apply.[101]

Katz shifted Fourth Amendment protection from places to people and introduced the language of a "reasonable expectation of privacy" to Fourth Amendment analysis. In later cases, however, the Court limited the application of the reasonable expectation of privacy by equating privacy with secrecy. The only significant limitation on

Ku, *supra* note 5, at 1369-72 (discussing general public use exception).

[99] *See supra* notes 90-93 and accompanying text.

[100] *See also* Greenwood v. California, 486 U.S. 35, 45 (1988) (approving warrantless search of garbage left in front of house); Oliver v. United States, 466 U.S. 170, 178-81 (1984). *Compare* California v. Ciraolo, 476 U.S. 207, 213 (1986) (holding warrantless use of imaging device from aerial flight over secluded backyard did not implicate Fourth Amendment), *with* Kyllo v. United States, 533 U.S. 27, 33 (2001) (holding warrantless use of thermal imaging device to scan interior of private home implicated Fourth Amendment).

[101] *See, e.g.*, Colb, *supra* note 5, at 120.

government authority remained at the threshold to the private home, despite the promise of *Katz* that the Amendment protects "people, not places." In many instances, the Court held that the Fourth Amendment did not apply, leaving law enforcement with no constitutional guidance for the exercise of their discretion. Congressional legislation filled the void created by the absence of guidance from the Court. Many of the bills were directed specifically at law enforcement's need for clear guidelines for the use of electronic surveillance.

B. Statutory Restrictions on Governmental Use of Electronic Surveillance

As mentioned earlier, one criticism of Fourth Amendment jurisprudence is the binary, all-or-nothing determination of whether a given action constitutes a search.[102] In addition to constitutional rulings, the field of electronic surveillance is also regulated by a comprehensive set of statutes. The statutory structure has supplemented the all-or-nothing approach with standards that permit varied degrees of intrusion based on a variegated showing of information by the government.[103] In the area of electronic surveillance, a pattern of action and reaction forged the legal framework. In passing turns, the legislature responded to the rulings of the judiciary and the judiciary interpreted the actions of the legislature.

1. Communications Act of 1934

An early example of the action and reaction pattern occurred with section 605 of the Federal Communications Act. Soon after *Olmstead v. United States*,[104] Congress passed the Communications Act of

[102] Amsterdam, *supra* note 5, at 385-86.

[103] The following discussion references: "Pen Registers and Trap and Trace Devices," 18 U.S.C. §§ 3121-3127 (2000 & Supp. V 2005); the "Stored Communications and Transactional Records Access," *id.* §§ 2701-2712 (2000 & Supp. V 2005); "Title III," *id.* §§ 2510-2522 (2000 & Supp. V 2005); "Wire and Electronic Communications Interception and Interception of Oral Communications," *id.*; and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 18, 26 and 50 U.S.C.).

[104] Recall that *Olmstead* reaffirmed the trespass rule in finding no Fourth Amendment protection against wiretaps. *See* Olmstead v. United States, 277 U.S. 438, 465 (1928). The issues were well-framed by the vigorous dissent of Justice Brandeis and the majority opinion of Chief Justice Taft. It is widely assumed that the

1934,[105] which regulated the use of telephone equipment and specifically ensured the security of communications transmitted electronically.[106] Section 605 of the Communications Act prohibited any person "receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication" from divulging or publicizing "the existence, contents, substance, purport, effect, or meaning" of the communication.[107] The Communications Act also prohibited the interception of any communication without the consent of the sender: "No person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any other person."[108] In essence, the Communications Act prohibited interception of wire communications, which, in principle if not in practice, eliminated the use of wiretaps from law enforcement's repertoire.[109]

2. Omnibus Crime Control and Safe Streets Act of 1968 ("Title III")

A second example of the action and reaction pattern occurred in 1968 with the Omnibus Crime Control and Safe Streets Act (also known as Title III). After the *Katz* and *Berger* decisions,[110] and in

Communications Act was passed as a congressional response to *Olmstead*. *See* Berger v. New York, 388 U.S. 41, 51 (1967) (noting, "Congress soon thereafter, and some say in answer to *Olmstead*, specifically prohibited the interception without authorization and the divulging or publishing of the contents of telephonic communications").

[105] Communications Act of 1934, ch. 652, 48 Stat. 1064 (codified as amended in scattered sections of 47 U.S.C.).

[106] 47 U.S.C. § 605(a) (2000).

[107] *Id.*

[108] *Id.*

[109] However, it is clear that J. Edgar Hoover's FBI used wiretaps extensively, keeping files on many noted figures, including Supreme Court Justices. SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 30, at 264; *see also* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 330 n.8 (Douglas, J., concurring) (listing recent reports of electronic surveillance); Daniel Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1273-74 (2004) (noting, in hindsight, fears of Justice Douglas that Supreme Court was bugged seem to have been correct). *See generally* DAVID GARROW, THE FBI AND MARTIN LUTHER KING (1981) (reporting on declassified documents detailing FBI's surveillance of Dr. King).

[110] *Berger* held that New York's wiretap statute failed to appreciate the extreme interest that was being encroached, and failed to take corresponding precautions mandated by the peculiarity requirement of the Fourth Amendment before permitting the wiretap intrusions, such as requiring exhaustion of other investigative techniques, requiring minimization of the intrusion to communications that were relevant to the

response to pressure from law enforcement groups interested in using electronic means to fight organized criminal enterprises,[111] Congress enacted Title III.[112] Title III relaxed the restrictions placed on law enforcement by the ban in section 605 of the Communications Act on all disclosure of intercepted communications.[113] Consistent with the elaborate protocols demanded in *Berger*, law enforcement could obtain, pursuant to Title III, a judicial order permitting the interception of certain electronic communications.[114]

Title III permitted the use of wiretaps only in the enforcement of specific and serious crimes.[115] Government agents had to follow detailed procedures before applying to a judge for an order authorizing the wiretap,[116] including providing the identity of the law enforcement officer seeking the order,[117] details of the particular offense under investigation,[118] a description of the location where the interception will occur,[119] a description of the type of communication to be intercepted,[120] and the identity of the subject of the investigation whose communications would be intercepted.[121] In addition, the application had to indicate that alternative investigative techniques have either failed, or are reasonably expected to fail.[122] Wiretaps

investigation, and limiting the time period for the intrusion. Berger v. New York, 388 U.S. 41, 44 (1967). Many of the concepts annunciated by the Court in *Berger* were incorporated into Title III. For a more detailed history of the role of *Katz* and *Berger* in the promulgation of Title III, see Solove, *supra* note 109, at 1275.

[111] *See Keith*, 407 U.S. at 310 n.9 (characterizing electronic surveillance and wiretaps as "the single most valuable weapon in law enforcement's fight against organized crime" (citing 117 CONG. REC. 14051 (1971) (testimony of Frank Hogan, Dist. Att'y of New York, New York))).

[112] Omnibus Crime Control and Safe Streets Act of 1968 (Title III), Pub. L. No. 90-351, 82 Stat. 212 (codified at 18 U.S.C. §§ 2510-2520 (2000)).

[113] 18 U.S.C. § 2517 (2000).

[114] *Keith*, 407 U.S. at 302 ("The Act represents a comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression. Much of Title III was drawn to meet the constitutional requirements enunciated by this Court in *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967).").

[115] For a list of the specified offenses, see 18 U.S.C. § 2516 (2000).

[116] For a list of the specific procedures, see § 2518 (2000).

[117] *Id.* § 2518(1)(a).

[118] *Id.* § 2518(1)(b)(i).

[119] *Id.* § 2518(1)(b)(ii).

[120] *Id.* § 2518(1)(b)(iii).

[121] *Id.* § 2518(1)(b)(iv).

[122] The Act requires a "full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." *Id.* § 2518(1)(c).

remain the most highly restricted form of electronic surveillance as they reveal the contents of the communications.[123] One noted commentator, Professor Orin Kerr, referred to wiretap orders as "Super Warrants" for the amount of information required for their issuance and the degree of minimization required during their execution.[124]

3. Foreign Intelligence Surveillance Act of 1978

The use of electronic surveillance in the espionage context created unique legal difficulties. For example, in *Keith*, the Court explicitly excluded from its holding the area of electronic surveillance of foreign powers.[125] The tension between the need to gather intelligence about foreign governments and the desire to restrain executive authority prompted Congress to act. In 1974, Congress passed the Privacy Act,[126] and in 1976 the Church Commission published its report to Congress, detailing the government's domestic surveillance programs and espionage activities.[127] The Foreign Intelligence Surveillance Act ("FISA")[128] filled the gap noted in *Keith* and created a legal mechanism for intelligence agencies to intercept the communications of foreign powers. FISA also authorized agents to intercept communications of "United States persons."[129] While FISA permitted intelligence agencies a free hand when intercepting communications of foreign powers, it required agents to obtain a court order for domestic interception of

[123] Policy groups generally supported legislative efforts to control electronic surveillance. For example, in 1971, the ABA proposed standards to govern the use of electronic surveillance. *See* ABA PROJECT ON STANDARDS FOR CRIMINAL JUSTICE, ELECTRONIC SURVEILLANCE § 4.1 (1971).

[124] Orin Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Wasn't*, 97 N.W. L. REV. 607, 620 (2003).

[125] United States v. U.S. Dist. Court (*Keith*), 407 U.S. 302, 315 (1972); *see supra* Part II.A.2.

[126] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2000)).

[127] Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, S. REP. NO. 94-755, at 332 (1976).

[128] Foreign Intelligence Surveillance Act (FISA) of 1978, tit. I, Pub. L. No. 95-511, 92 Stat. 1976 (codified as amended in scattered sections of 50 U.S.C.).

[129] FISA defines a "United States person" as "a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States which is not a foreign power." 50 U.S.C. § 1801(h)(4)(i) (2000).

the communications of a United States person.[130] Following the advice of Justice Powell in *Keith*,[131] FISA created special courts to review applications for electronic surveillance, including wiretaps that reveal the contents of communications.[132]

4. Electronic Communications and Privacy Act

Recognizing the gap opened by the adoption of new technologies, such as email, Congress revisited Title III in 1986 with the Electronic Communications and Privacy Act ("EPCA"), which amended Title III and separated electronic surveillance into three sections: the Wiretap Act (covering interception of wire communications), the Stored Communications Act ("SCA") (covering communications stored during or after transmission), and the Pen Register Act (covering the use of pen registers and trap and trace devices).[133] The amendments to Title III restrict these forms of electronic surveillance to persons authorized by a court order, yet do not require a probable cause showing before the order will issue.[134] For example, a pen register order merely required that a government attorney certify to the court that the information requested is relevant to a criminal investigation.[135]

EPCA also covered email. Under the SCA, email was protected as an electronic or wired communication; however, an email message stored on an Internet Service Provider ("ISP") server for more than 180 days receives less protection, and can be obtained through a mere

[130] *Id.* § 1802(b) (2000); *see also id.* § 1801(h)(4).

[131] United States v. U.S. Dist. Court (*Keith)*, 407 U.S. 297, 323 (1972) ("It may be that Congress, for example, would judge that . . . the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court . . . ."); *see supra* notes 61-66 and accompanying text (discussing *Keith*).

[132] FISA was amended by the USA PATRIOT Act to increase the number of judges on the FISA Court from seven to 11. 50 U.S.C. §1803(a) (2000).

[133] The scope of information covered by the Pen Register Statute was expanded by the USA PATRIOT Act, and now includes "dialing, routing, addressing or signaling information"; however, any "content" information shall not be disclosed under a pen register order. 18 U.S.C. § 3127(3)-(4) (2000). The USA PATRIOT Act amended Title III to include Internet communications. Thus the envelope information of a pen register includes Internet protocol addresses ("IP"), uniform resource locators ("URL"), and other addressing information. *Id.*

[134] *Id.* § 2703 (2000) (discussing stored communications); *Id.* § 3122 (2000) (discussing pen registers).

[135] *Id.* §§ 2510, 2516, 3122(a)(2) (2000).

application to a court.[136] Notably, the dominant email platform in 1986 did not contemplate the storage of user email on the ISP server for more than a very short time. Within a few years after the enactment of the SCA, the dominant protocol shifted to a platform where email was stored on the ISP server, rather than on the user's machine.[137] Thus, if Congress intended to provide a greater degree of protection to active emails, it failed to keep pace with technological innovation.[138]

5. Communications Assistance for Law Enforcement Act of 1994

In response to law enforcement's perceived need for assistance in coping with new communications technology, Congress enacted the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), which required ISPs and telecom providers to allow authorized government agents to access communication networks for

[136] *Id.* § 2703(a) (2000).

[137] Though not the subject of this Article, it is interesting to note the development of email technology.

In Internet Engineering Task Force ("IETF") documents referred to as Requests for Comments ("RFCs"), the group maintains a record of developments in various fields. In a the area of networking, which includes email systems, Steven Crocker submitted RFC 1 on April 7, 1969, describing a system for delivering messages divided into packets over a network. This system evolved into an email protocol. The prevailing network protocol for email in 1986 was Post Office Protocol, or POP, introduced on RFC 918 by J.K. Reynolds in October, 1984, and revised substantially by a group from ISI in February 1985. In July 1988, Mark Crispin submitted RFC 1064, which described IMAP (Internet Message Access Protocol) version 2, which was the first publicly distributed version of the application. Most current email applications run IMAP version 4. The principal advantage of the IMAP over the POP lies in the use of a systems server to access and store messages rather than the individual user machine.

Crispin describes disadvantages of POP. IMAP stores messages on the server rather than on the user's workstation, thus limiting the damage when an individual user suffers a hardware failure, which in theory, would occur less frequently, and less catastrophically, to a system server. *See* M. Butler et al., *Post Office Protocol – Version 2* (Feb. 1985), http://www.tools.ietf.org/html/rfc937; M. Crispin, *Interactive Mail Access Protocol – Version 2* (July 1988), http://www.tools.ietf.org/html/rfc1064; Steve Crocker, *Host Software* (Apr. 7, 1969), http://www.tools.ietf.org/html/rfc1; J.K. Reynolds, *Post Office Protocol* (Oct. 1984), http://www.tools.ietf.org/html/rfc918/; J. Rice, *Interactive Mail Access Protocol – Version 3* (Feb. 1991), http://www.tools.ietf.org/html/rfc1203; *see also* Internet Message Access Protocol, http://www.en.wikipedia.org/wiki/Internet_Message_Access_Protocol (last visited Jan. 9, 2008) (describing Internet Message Access Protocol).

[138] The Sixth Circuit recently held that email deserved a higher degree of constitutional protection; however, the decision is currently pending en banc review. Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), *vacated and reh'g en banc granted*, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 9, 2007).

the purpose of conducting electronic surveillance.[139] CALEA also prohibited the interception of cordless phone calls and required ISPs to disclose encryption keys to the government.[140] In reaction to concerns about the expansion of the power of the executive branch, CALEA specifically limited the use of certain technologies. For example, CALEA stated that information obtained through pen registers and trap and trace devices "shall not include any information that may disclose the physical location of the subscriber."[141] Significantly, the Director of the Federal Bureau of Investigation testified before Congress as to the effect of the CALEA legislation. FBI Director Louis Freeh stated that the proposed legislation "ensures the maintenance of the status quo" as to the legal authority for wiretaps and pen/traps, that the bill "does not enlarge or reduce the government's authority" for such electronic surveillance, and that the proposed legislation "relates solely to advanced technology, not legal authority or privacy."[142]

6. USA PATRIOT Act

In October 2001, Congress passed the USA PATRIOT Act, and in March 2006 Congress renewed certain provisions of the Act.[143] The USA PATRIOT Act amended numerous statutory provisions and is best understood as a massive list of minor amendments to existing statutes rather than as a new piece of legislation.[144] The major sections of the Act relaxed the standards required to obtain a surveillance order on a U.S. person, authorized "roving" surveillance orders, permitted greater exchange of information between the historically segregated intelligence and law enforcement communities, and allowed greater

[139] Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended in scattered sections of 47 U.S.C.).

[140] *Id.* § 103(b)(3).

[141] 47 U.S.C. § 1002(b)(2)(B) (2000); *see also id.* § 1002(a)(2).

[142] *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearing Before the Subcomm. on Technology and Law of the S. Judiciary Comm. and the Subcomm. on Civil and Constitutional Rights of the H. Judiciary Comm.*, 103d Cong. 2d 2, 28 (statement of Louis Freeh, FBI Director), *available at* http://w2.eff.org/Privacy/Surveillance/CALEA/freeh_031894_hearing.testimony.

[143] USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, (codified as amended in scattered sections of 26 U.S.C.); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192, 210 (2006). Although the USA PATRIOT Act followed *Kyllo v. United States*, 533 U.S. 27 (2001), the events of September 11, 2001, were the primary impetus to the USA PATRIOT Act.

[144] USA PATRIOT ACT § 1, 115 Stat. 272, 272-75.

authority to search business records.[145] With respect to electronic surveillance, the major work of the Act was to bring Internet communications within the scope of Title III by requiring a court order for the government to conduct surveillance, while prohibiting non-governmental entities from conducting Internet surveillance.[146]

In addition, the USA PATRIOT Act amended the FISA statute by changing the operating mandate from one exclusively directed to foreign intelligence to one aimed more broadly at law enforcement.[147] The USA PATRIOT Act expanded the definition of pen registers and trap and trace devices by including "routing and signaling information."[148] The Act also amended EPCA by permitting easier access to voicemail and to stored electronic communications.[149] Under the previous statutory restriction, voicemail fell into the same category as an active telephone conversation and required a wiretap order. The amended statute placed voicemail into the category of stored communications, which required an "ordinary" warrant.[150]

7. Summary of Statutory Limits on Electronic Surveillance

The absence of significant constitutional limitations in the area of electronic surveillance and the heightened concern over the invasive nature of the surveillance has led to a comprehensive statutory framework. Legislative action frequently followed on the heels of Supreme Court decisions. Commentators have noted several reasons for this phenomenon: the Supreme Court cases focused public attention on an issue, and the Supreme Court decisions invariably included vigorous dissents which frame the issues well.[151] The high level of legislative regulation can be interpreted as a reflection of the

[145] *Id.*

[146] The USA PATRIOT Act is divided into ten sections, one of which, Title II – Enhanced Surveillance Procedures, deals primarily with surveillance. USA PATRIOT ACT §§ 201-25, 115 Stat. 272, 278-96.

[147] Specifically, section 218 of the Act amended FISA by striking "the purpose" and inserting "a significant purpose." USA PATRIOT ACT § 218, 115 Stat. 272, 291.

[148] Specifically, section 216 of the Patriot Act dealt with pen registers and trap and trace devices. USA PATRIOT ACT §216(c)(2)(A), 115 Stat. 272, 288-90 (amending 18 U.S.C. § 3127).

[149] USA PATRIOT ACT §§ 209, 210, 115 Stat. 272, 283 (amending 18 U.S.C. §§ 2510, 2703).

[150] *Id.*

[151] SOLOVE, ROTENBERG & SCHWARTZ, *supra* note 30, at 262-63; *see also* Swire, *supra* note 17, at 917.

deep concern of the People for the integrity of their personal security.[152]

II. RECENT DEVELOPMENTS

Technological advances in the area of communications have greatly increased the capacity to create, distribute, search, and share information. In person-to-person communication, electronic communications have replaced letters and packages, and increasingly, voice communications.[153] Many Americans shop, pay their monthly bills, and conduct financial transactions electronically. Numerous Internet companies offer social networking or dating services where interested parties meet and communicate via email;[154] electronic communications via these social networking services have replaced face-to-face conversations. Traditional wire (landline) services now compete with Voice-over-Internet Protocol ("VoIP") services that digitize audio signals, effectively changing spoken conversations into electronic messages.[155] Commercial enterprises, such as DoubleClick, ChoicePoint, and Lexis-Nexis, track Internet and consumer spending habits, creating extensive data profiles for American consumers. In each of these scenarios, personal information is transmitted over the

[152] One commentator has suggested that the legislature, and not the courts, are properly situated to regulate electronic surveillance. Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 804-06 (2004) ("[C]ourts should place a thumb on the scale in favor of judicial caution when technology is in flux, and should consider allowing legislatures to provide the primary rules governing law enforcement investigations involving new technologies.").

[153] A recent poll found that 70% of American adults use the Internet (approximately 141 million Americans). Popular uses of the Internet include email (91%), searching for general health information (79%), obtaining information regarding a specific medical condition or personal situation (58%), and banking online (43%). *See* Pew Internet & American Life Project, Internet Activities, http://www.pewinternet.org/trends/Internet_Activities_1.11.07.htm (last visited Jan. 9, 2008).

[154] *See, e.g.*, Facebook, http://www.facebook.com (last visited Jan. 9, 2008); FriendFinder, http://www.friendfinder.com (last visited Jan. 9, 2008); Match.com, http://www.match.com (last visited Jan. 9, 2008); MySpace, http://www.myspace.com (last visited Jan. 9, 2008). MySpace claims more than 100 million subscribers. Myspace, *supra*. Match.com claims more than 15 million subscribers and more than 500,000 "matches." Match.com, *supra*.

[155] The difference between landline and VoIP technologies is not as great as it might initially appear. Landline communications are converted from analog to digital and transferred over Internet data networks, then reconverted to analog signals for the "last mile." This technology has greatly reduced the actual cost of long distance calling.

Internet in electronic form. En route, the electronic communications are routed through ISPs and are stored, for a time, on their servers. The conversion, through the adoption of new technology, of oral communications to stored electronic communications has profound legal consequences because the legal framework treats stored communications differently from oral communications.[156]

The next section describes the technology used in the Internet and in cell phones. The second section of this Part examines the particular legal challenges presented in the Pen Register Decisions and the NSA Cases. The cases lead to a discussion of whether our current legal framework adequately protects the collective interests of the People and promotes the right to be secure.

A. Technological Advances

1. Basic Internet Architecture

Any discussion of current technology should begin, and probably end, with the Internet. The origins of the Internet can be traced to a communications network established by the Department of Defense and the Computer Science Network. The World Wide Web standard stems from collaboration between the Massachusetts Institute of Technology and CERN, Europe's particle accelerator facility.[157] The Internet is comprised of a network of fiber-optic cables that connect end users to one another. ISPs connect individual users through the network of connections to other users, but all ISPs are not equal.[158] The largest telecommunications providers in the world are the giants

[156] Specifically, under the Stored Communications Act ("SCA"), stored communications are not subject to the same type of warrant requirement as the interception of a voice call under Title III. Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 462 (5th Cir. 1994) (finding "Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage'").

[157] ARPANET stands for Advanced Research Project Agency Network. Other precursors of the modern Internet include: CSNET, or Computer Science Network (linking computer science departments); NSFNET, the National Science Foundation Network; BITNET, the Because It's Time Network, which began as a network between CUNY and Yale which then expanded; CREN, the Corporation for Research and Education Network; UUNet and USErNet, developed by Duke University to use a Unix to Unix Communications Protocol (UUCP); and IBM's internal network. *See* About W3C, http://www.w3.org/consortium/ (last visited Jan. 9, 2008).

[158] "Peering" is commonly known as "Settlement Free Interconnection." The degree to which ISPs engage in peering divides providers into four tiers. Tier 1 ISPs "peer" with all other ISPs without paying access fees.

of the Internet; in effect their networks of cables and connections are not connected to the Internet, they are the Internet.[159] If the Internet is analogized to a road structure, the "Tier 1" provider cables are the superhighways.[160]

The Internet is significant in several ways: First, the type of information flowing across the Internet includes a spectrum from mundane advertising to intimate personal details of relationships, health, and financial information. Second, many types of communication are sent in the same way — converted to digital bits, encoded in layers of information, and sent in packets to the destination.[161] This convergence of communication makes it difficult to create distinctions in the type or content of communications. While it might be easy to say a billboard is a type of communication that is different from a whispered conversation and deserving of less legal protection, on the Internet every piece of information, whether an advertisement or a personal health record, is a qualitatively identical bit-stream. It is difficult to distinguish one binary bit-stream from another. Third, the architecture of the Internet places an inordinate amount of control of information in the hands (or cables, as the case may be) of just a few providers. The top-tier ISPs handle an incredible amount of information and provide a ready access point for interception, should one be so inclined.

With respect to the Internet (and telephone), courts have frequently tried to analogize and distinguish among the new technologies and the known entities of pen, paper, and postal system.[162] Thus, a pen

[159] The Tier 1 ISPs control most of the high traffic trunk lines which evolved from telecommunications lines.

[160] Each day the AT&T Corporation processes approximately 300 million voice calls and 4000 terabytes of data, an amount 200 times greater than the information contained in all of the books in the Library of Congress. *See* Declaration of J. Scott Marcus at 7, Hepting v. AT&T, 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. C-06-672 UWR).

[161] Information is transferred over the Internet in bundles called "packets." When a sender sends a digital message over the Internet, the message is broken into packets and sent independently to the destination, where the constituent pieces of the message are then reassembled.

[162] In *Warshak v. United States*, the government attempted, unsuccessfully, to extend the "postcard" analogy to email. The Sixth Circuit affirmed the decision of the district court, which held that there was a reasonable expectation of privacy in email, such that a warrant was required to obtain access to the contents of the email communication. However, the Sixth Circuit recently granted en banc review, vacating the earlier decision and restoring the case to the appellate calendar. Warshak v. United States, 490 F.3d 455, 469-76 (6th Cir. 2007), *vacated and reh'g en banc granted*, No. 06-4092, 2007 U.S. App. LEXIS 23741 (6th Cir. Oct. 7, 2007).

register has been described as accessing "envelope" information, however, the information actually accessed by a pen register is significantly more detailed than the information that appears on the outside of a mailed envelope.[163] The attempt to categorize modern communications based on an antiquated mail delivery system inevitably fails to properly recognize that Internet-based communications differ significantly from the technologies they replaced. Convergence between telephone, cable television, and ISPs demonstrates the blurring distinctions between traditional electronic media and Internet-based communications. In sum, the Internet presents a new environment because of the ubiquity, the vast quantity, and the absence of clear distinctions in the type and content of the information it contains.

2. Cell Phone Technology

The technology of pen registers has progressed significantly since 1971, when the Supreme Court decided *Smith v. Maryland*.[164] In *Smith*, the Court declined to extend constitutional protection to pen register devices relying, in part, on the limited information obtained from a pen register.[165] The device, according to the Court, "does not indicate whether calls are actually completed."[166] A "traditional" pen register provides a list of numbers called; a trap and trace device provides a list of numbers from incoming calls.[167]

[163] The entire analogy may depend on the faulty premise that messages sent through the postal system in a sealed envelope cannot be legally opened and read by the government (absent a warrant). However, President Bush, in a "signing statement," noted that his interpretation of the Postal Accountability and Enhancement Act provided for "opening of an item of a class of mail otherwise sealed against inspection." President's Signing Statement on Postal Accountability and Enhancement Act, H.R. 6407, 1 PUB. PAPERS 2196 (Dec. 20, 2006), *available at* http://www.whitehouse.gov/news/releases/2006/12/20061220-6.html. It appears, according to President Bush, there is no reasonable expectation of privacy in "a class of mail otherwise sealed against inspection." *Id.*

[164] 442 U.S. 735 (1971); *see supra* Part II.A.3.

[165] 442 U.S. at 745.

[166] *Id.* at 736 n.1.

[167] 18 U.S.C. § 3127 (2000) defines "pen register" as a "device or process which 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.* § 3127(3). A "trap and trace device" is defined as a "device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication . . . ." *Id.* § 3127(4). The statute expressly states that pen registers and trap and trace

Current cell phone technology permits the acquisition of significantly more information than a traditional pen register placed on a landline.[168] A pen register on a cell phone with "cell site" tracking provides not only envelope information regarding the numbers dialed, but also very useful information regarding the location of the cell phone (and presumably the location of the owner of the phone). As a cell phone moves, its signals are picked up by different cell phone towers located within close geographic proximity. Precise locations can be determined by analyzing signals from two or more towers. Through relatively simple trigonometric calculations (performed by a computer, of course), the precise location of the transmitting device can be determined either by looking at the angle of signal reception from two antennae towers, or by calculating the difference in signal arrival at stationary antennae towers.[169] By examining the strength of the signal and the angle of reception received by different cell phone towers, the precise location of the cell phone can be determined.[170] In effect, every cell phone can be converted into an individual tracking device, accessible in real time.[171] Further, when the phone is turned on, it will send a signal to establish a link to the network in order to receive incoming calls. This initial

devices "shall not include the contents of any communication." *Id.* § 3127(3)-(4).

[168] Pursuant to the Wireless Communications and Public Safety Act of 1999, all cellular phones are equipped with E911 technology, essentially a built-in GPS tracking device that can provide exact geographical location information. The law encouraged deployment of a seamless 911 safety network; however, the technology provides the convenient capability to track the precise geographic location of any cellular phone, and presumably, its owner in real time. *See* Wireless Communication and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286, 1287 (codified at 47 U.S.C. § 615 (2000)).

[169] Note, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308-16 (2004); *see also Smith*, 396 F. Supp. 2d 747, 751, 755 n.12 (S.D. Tex. 2005).

[170] Note, *supra* note 169, at 308-09.

[171] If the tracking device is placed on a vehicle and the monitoring occurs while the vehicle is on public roads, then no warrant is required. *See* United States v. McIver, 186 F.3d 1119, 1127 (9th Cir. 1999) (finding no warrant necessary for installation of GPS tracking device on vehicle under rationale of *United States v. Knotts*); *Smith*, 396 F. Supp. 2d at 752; *Orenstein II*, 396 F. Supp. 2d 294, 322 (E.D.N.Y. 2005); *cf.* United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006) (permitting evidence obtained from tracking device, but suppressing evidence obtained from device while in defendant's home). *Compare* United States v. Knotts, 460 U.S. 276 (1983) (holding that when information could have been obtained through visual observation, no warrant is required for electronic monitoring), *with* United States v. Karo, 468 U.S. 705 (1984) (holding that when location is not open to visual surveillance, warrantless monitoring violates Fourth Amendment).

passive connection can also be used to monitor the location of the phone when it is turned on, but not in use, using the same techniques as are used during a phone call.[172]

B. The Pen Register Decisions

In August of 2005, an Assistant United States Attorney submitted a standard ex parte application for a pen register to Magistrate Judge Orenstein in the Eastern District of New York.[173] Nearly identical to another application that had been granted just a few months before, this application requested "disclosure of the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls), and if reasonably available, during the progress of a call, for the Subject Telephone."[174] The government sought location information because the "geographic location of the Subject Telephone derived from cell site information" could be used to "corroborate the observations of surveillance agents" and "verify the identification and location of the user of the Subject Telephone."[175]

In a decision of first impression, Magistrate Judge Orenstein denied the portion of the August application that requested location information via the pen register.[176] The government filed a motion for reconsideration, and in a longer, more thorough decision, dated October 24, 2005, Magistrate Judge Orenstein again denied the government access to cell site information.[177] Over the ensuing twelve months, through October 2006, fifteen decisions were published in various federal districts around the country on the issue of government applications for pen registers with cell site location information.[178] Of the fifteen decisions, eleven have denied relief and four have granted relief. Although district court judges reviewed two of these decisions, no case has been appealed.

---

[172] Dialing the cell phone number will trigger the phone to connect to the closest network through the closest antennae. When agents lose contact with a target, they use a technique of dialing the number but hanging up before the phone rings, which will prompt the phone to signal the closest antennae, revealing the location of the phone. In *United States v. Forest*, 355 F.3d 942, 947-52 (6th Cir. 2004), the court noted this technique, but did not rule on its propriety.

[173] *Orenstein I*, 384 F. Supp. 2d 562, 563 (E.D.N.Y. 2005).

[174] *Id.*

[175] *Id.* at 564.

[176] *Id.*

[177] *Orenstein II*, 396 F. Supp. 2d 294, 294 (E.D.N.Y. 2005).

[178] *See* cases cited *supra* note 16.

There is no constitutional barrier to a warrantless pen register interception because the Supreme Court held, in *Smith*, that a pen register interception is not a search: a caller has no reasonable expectation of privacy in the numbers dialed because the dialing information had already been exposed in the course of transmission to the telephone carrier.[179] Although a pen register is not a search within the meaning of the Fourth Amendment, government agents must obtain judicial approval in order to comply with the Pen Register Act.[180] To obtain orders for pen register and trap and trace devices, whether on landlines or on cell phone numbers, a government agent must present to a magistrate a certification that the target number is relevant to an ongoing investigation.[181] Clearly, the information required to obtain a pen register order falls well below the probable cause standard required for a warrant.

The government need not obtain prior approval for the use of a tracking device in some circumstances. Under the rationale and holding of *United States v. Knotts*,[182] an electronic device that tracks movements on public roads is not a search and does not require a warrant. However, under the holding of *United States v. Karo*,[183] if the agents continued to monitor the tracking device in the target's home, the intrusion would trigger the Fourth Amendment's warrant requirement.[184] Personal tracking devices differ substantially from vehicular tracking devices — the high probability that an individual tracking device will enter the protected domain of the private home essentially mandates the use of a traditional warrant.[185]

The Pen Register Decisions analyzed whether the government was authorized to obtain additional location information merely by presenting a certification that the target was relevant to an ongoing criminal investigation. Before 2005, courts routinely granted government applications for cell site tracking under Title III's pen register provision.[186] The applications were necessarily made ex parte;

[179] Smith v. Maryland, 442 U.S. 735, 744 (1971).

[180] 18 U.S.C. § 3122(a)(1) (2000).

[181] *Id.*

[182] 460 U.S. 276, 282 (1983).

[183] 468 U.S. 705, 716 (1984).

[184] *Id.* at 717.

[185] Rule 41 authorizes a warrant based on probable cause. *Smith*, 396 F. Supp. 2d 747, 752 (S.D. Tex. 2005) ("A Rule 41 probable cause warrant was (and is) the standard procedure for authorizing the installation and use of mobile tracking devices.").

[186] Indeed, in several opinions, judges candidly admit to granting nearly identical

the owner of the target telephone had no immediate knowledge of the government's action. Further, the target had no opportunity to challenge the government's action unless the subject telephone belonged to the target of the investigation and the government sought to introduce evidence of the cell location at trial.[187]

1. The Hybrid Theory and the Instantaneous Storage Theory

The government's position has been described as the "hybrid theory" because it combined authority from two different statutes in a manner that allowed the government to accomplish actions that neither statute, standing alone, would permit.[188] The government initially faced the hurdle presented by the language of CALEA, which stated that information obtained through pen registers and trap and trace devices "shall not include any information that may disclose the physical location of the subscriber."[189] In response, the government argued that the Pen Register Statute, combined with CALEA, allowed the government to obtain the location information.[190] Under this theory, a Pen Register order, combined with an order pursuant to SCA,[191] provided sufficient authority to obtain cell site tracking information. The argument progressed as follows: (1) Cell site location information fell within the pen register definition, which was amended by the USA PATRIOT Act; (2) CALEA prevented disclosure of location information when the government has only a pen/trap order; (3) if the government had additional authority, then CALEA did not bar the government from obtaining location information; (4) an SCA order permitting the government to obtain "record[s] or other information pertaining to a subscriber . . . (not including the contents of communications)" upon a showing of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation," provided

applications in the months prior to the decision. *See, e.g.*, *Orenstein I*, 384 F. Supp. 2d 562, 566 (E.D.N.Y. 2005) ("I acknowledge that I have previously granted applications for similar relief, as recently as April 1, 2005, without questioning the legal basis for doing so or suggesting that there might be none.").

[187] Disclosure to the subscriber of the existence of a pen register is specifically prohibited. 18 U.S.C. §3123(d) (2000 & Supp. V 2005).

[188] *Smith*, 396 F. Supp. 2d at 761-63; *Orenstein II*, 396 F. Supp. 2d 294, 315-17 (E.D.N.Y. 2005).

[189] 47 U.S.C. § 1002(b)(2)(B) (2000); *see also id.* § 1002(a)(2) (2000).

[190] *Smith*, 396 F. Supp. 2d at 761.

[191] 18 U.S.C. § 2703(d) (2000).

the additional authority required by CALEA; and therefore, (5) the "records or other information" authorized by the § 2703(d) order may be collected prospectively through a pen/trap device.[192]

In the alternative, the government presented the "instantaneous storage theory," which asserted that because the information collected by a pen register was stored instantaneously on the ISP's server, there was no practical difference between an order permitting disclosure of historical information under § 2703 and an order permitting disclosure of prospective information pursuant to a pen/trap order.[193] Specifically, the government argued that "the same datum that is prospectively covered by a disclosure order is a 'record' by the time that it must be turned over to law enforcement."[194]

According to the analysis in *Orenstein II* and *Smith*, the cell site transmission information is not a wire or electronic communication pursuant to Title III. *Orenstein II* distinguished the disclosures requested by the government and the disclosures authorized according to two criteria: the level of information required at the time of the order and the point in time when the government could obtain the information.[195] The court noted that the government could, pursuant to § 2703, acquire historical cell site information that the provider had stored electronically.[196] In addition, the court acknowledged that the government could obtain a real time tracking device for any individual, even if the government wanted to use the target's cell phone as the tracking device and the target's cell phone service provider as the monitoring system. However, that information would require a warrant pursuant to Federal Rule of Criminal Procedure 41 ("Rule 41").[197]

Further, the court suggested that if the government's proposal was to acquire the cell site information directly, rather than through disclosure by the provider, its actions might be wholly outside the limits of § 2703.[198] There was disagreement over whether a tracking

---

[192] *Smith*, 396 F. Supp. 2d at 761.

[193] 18 U.S.C. § 2703; *Orenstein II*, 396 F. Supp. 2d at 312.

[194] *Orenstein II*, 396 F. Supp. 2d at 312.

[195] *Id.*

[196] *Id.*

[197] *Id.* at 313. "[T]he difference between the acquisition of historical evidence about a person's movements and the prospective, real-time tracking of that person . . . is an important one, Congress has empowered the government to satisfy its investigative needs upon a showing of probable cause . . . ." *Id.*

[198] *Id.* at 314. The court used the term "intercept" to describe a situation where the government itself was acquiring the information, rather than using the disclosure mechanism available through § 2703. *Id.* at 314 & n.20.

device required a warrant pursuant to Rule 41,[199] and Magistrate Judge Orenstein noted that the Wireless Communication and Public Safety Act of 1999 prohibited the disclosure of call location information without the consent of the subscriber.[200] In sum, the government could acquire all of the information it requested, but it had to make a greater showing — essentially meeting the probable cause standard required for a warrant.[201]

2. Strategic Ex Parte Litigation

The Pen Register Decisions arose from an ex parte application by the government for an order permitting electronic surveillance where the interests of the opposing party were obviously unrepresented. The government and its attorneys must have confronted the issue of whether to develop a litigation strategy to "win" in a situation where the opposing side did not even have notice of the action of the government. In such a procedural posture, it might appear unseemly or unfair to develop and execute a litigation strategy.

The evidence from the case, however, demonstrates that the government pursued a litigation strategy aimed at gaining judicial momentum for the position that cell site location information could be obtained through a pen register application. The strategy had at least two prongs of attack: (1) gradually build judicial momentum in support of the government's position, and (2) avoid negative appellate precedent. First, the government would gradually increase the scope of the information requested, beginning with applications requesting cell site information from only a single tower and only at the time of call initiation. Then, once the courts ruled favorably on the issue of single tower information, the government would expand the scope of the applications to include multiple tower information, and ultimately to applications requesting multiple tower information in real time whenever the cell phone is turned on. In one decision, the court explicitly noted the government's legal strategy.[202]

---

[199] *Id.* at 323; *see also Smith*, 396 F. Supp. 2d 747, 758 (S.D. Tex. 2005) ("Because the government cannot demonstrate that cell site tracking could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking under 18 U.S.C. § 3117, which routinely require probable cause.").

[200] *See Orenstein II*, 396 F. Supp. 2d at 323; *see also* Wireless Communication and Public Safety Act of 1999, Pub. L. No. 106-81, 113 Stat. 1286.

[201] *Orenstein II*, 396 F. Supp. 2d at 321-22.

[202] *Feldman*, 415 F. Supp. 2d 211, 218 n.5 (W.D.N.Y. 2006). The court cited to a transcript of the hearing where the government attorney candidly admitted that the

The second prong of the litigation strategy appears to involve a calculated effort to avoid creating unfavorable precedent from higher courts. Notably, the government has not appealed any of the decisions to a court of appeal, despite specific requests from several lower court judges for guidance on the issue. [203] Professor Kerr described the execution of a similar litigation strategy at the Department of Justice: when a district court ruled against the government on a surveillance

practical considerations favored getting to "floor one," even though the argument presented would logically permit acquisition of much more information. In this case, the government had made the argument that location information was clearly "signaling" information under the Pen Register statute, to which the government was entitled under the SCA. However, the government had only requested "general location information" rather than specific "triangulation" information. The court noted that the government's argument, if valid, would apply equally to general and specific location information. Why, then, was the government only requesting general information?

> Court: If your argument makes sense, why doesn't it make sense for all the information you can collect?
>
> AUSA: Well there's a couple of practical things going on. One, we're before magistrate judges that are the gatekeepers — we're trying to convince them that the government isn't being some ruthless, overbearing entity — we're trying to be reasonable. So, therefore, if we can get the magistrate's ear and we don't have to fight this fight a zillion times, we'll back off. If you have this internal radar that's going "privacy interest, privacy interest," okay, we'll back off. But is it possible the argument could be made that we could be here on another day having gotten to floor one and now we're trying to get to floor two? Yes. Has that been suggested by anyone? Absolutely not.
>
> Court: In fact, you're telling me that the word you're getting is to stop at the general location?
>
> AUSA: . . . There's a common sense decision that says if we want to do this higher step, if we want to go to triangulation, we're going to have a hell of a fight, if we think we have a fight now, we'll have a heck of a fight on our hands because then we're on slippery ground, because there's no bedrock statute that says this is not a privacy concern as far as the courts are concerned in terms of a probable cause standard.

Id.

[203] *Id.*; *Orenstein I*, 384 F. Supp. 2d 562, 566 (E.D.N.Y. 2005) ("If the government intends to continue seeking authority to obtain cell site location information in aid of its criminal investigations, I urge it to seek appropriate review of this order so that magistrate judges will have more authoritative guidance in determining whether controlling law permits such relief on the basis of the relaxed standard set forth in 18 U.S.C. § 2703, or instead requires adherence to the more exacting standard of probable cause."); *Orenstein II*, 396 F. Supp. 2d at 327 ("I continue to urge the government to seek appropriate review of my decision in a forum that can provide more authoritative guidance on this important matter.").

issue, the Department of Justice decided to "keep quiet" about the court's unpublished decision.[204] The appearance of a litigation strategy suggests that the executive branch had already resolved the balance between the need for information relevant to law enforcement purposes and the legal limitations on governmental intrusions into the lives of the People, and that it had no interest, desire, or need for judicial review of its decision.

3. Summary of the Pen Register Decisions

There seems to be some consensus, though no unanimity, among courts that the statutes do not permit the government to obtain cell site information through a pen register application.[205] The cell site tracking process provides information beyond that which was authorized by the pen register exception under Title III and, therefore, courts must determine whether the targets of the investigation have a reasonable expectation of privacy in the additional undisclosed location information. Most of the decisions appear to have limited the government orders to information that could have been obtained in a traditional pen register.

These decisions are curious for several reasons. First, they offer a glimpse into the ex parte process through which the government obtained orders for pen registers. Second, it appeared that prior to the *Orenstein* decisions, the applications were routinely granted. In fact, Magistrate Judge Orenstein candidly admitted that he had previously granted similar applications "without questioning the legal basis for doing so or suggesting that there might be none."[206] At an ex parte proceeding, which is necessarily secret, there is no opportunity to challenge the practice unless the government sought to introduce evidence obtained from cell site tracking at a trial and a defendant

[204] Kerr, *supra* note 124, at 633-36 ("Within the criminal division of the DOJ, a sense emerged that the best approach was to keep quiet about Judge Trumbull's decision, which it did, as the DOJ has never shared Judge Trumbull's unpublished decision with the public.")

[205] The current count includes 15 reported opinions from 11 magistrates and four district judges. The district judges are split, with Judge Adelman from the Eastern District of Wisconsin joining Judge Lee from the Northern District of Indiana in denying the government's applications, and Judge Kaplan from the Southern District of New York joining Judge Rosenthal from the Southern District of Texas in granting the government's applications. The magistrates are split eight to three against the government's position. *See Kaplan*, 460 F. Supp. 2d 448, 451 (S.D.N.Y. 2006) (reviewing outcomes of previous decisions).

[206] *Orenstein I*, 384 F. Supp. 2d at 566.

challenged the admissibility of such evidence. [207] As a practical matter, the government may choose not to introduce evidence stemming directly from the cell site tracking, as the real utility of the location information lies at the investigation stages, not at the trial stage. Further, the target of the cell site pen register may not be the target of the criminal investigation. It would be difficult to challenge, in a motion to suppress, electronic surveillance of a third person, such as a friend or family member. Third, there is no record of a government appeal, even though a healthy debate existed among magistrates and district judges.[208]

Currently, it appears unlikely that an appellate court will address this issue. A number of possible avenues could resolve the issue: (1) the Department of Justice might be so concerned about the constitutional implications of the practice that they will cease using this type of surveillance, or they will only pursue this type of surveillance when they have sufficient information to meet the probable cause standard; (2) the district courts might realize that the Department of Justice was correct and will approve future applications accordingly; (3) the Department of Justice might direct future orders to courts friendly to their arguments; or (4) Congress might intervene and amend the statute, rendering the issue moot.

[207] *Kaplan*, 488 F. Supp. 2d 448 (S.D.N.Y. 2006) (suggesting proper venue for addressing Fourth Amendment issue would be during suppression hearing after filing of criminal indictment).

[208] District Judge Adelman of Wisconsin reviewed and upheld the findings of a magistrate who had denied the government's application. *Adelman*, No. 06-Misc-004, 2006 U.S. Dist. LEXIS 73324, at *2 (E.D. Wis. Oct. 6, 2006), *affirming In re* United States, 412 F. Supp. 2d 947 (E.D. Wis. 2006) (Callahan, Magis. J.). On the other hand, Judge Lewis Kaplan of the Southern District of New York reviewed and overturned the decision of Magistrate Peck, who had denied the government's application. *Kaplan*, 460 F. Supp. 2d 448, 454 (S.D.N.Y. 2006); *Peck*, No. 06-Crim-Misc-01, 2006 U.S. Dist. LEXIS 11747, at *1 (S.D.N.Y. Mar. 2, 2006). Magistrate Judge Smith of Texas and Magistrate Judge Peck of New York expressed the hope that their decisions would be reviewed by higher courts. *Peck*, 2006 U.S. Dist. LEXIS 11747, at *7 ("I recommend that the government seek review of this issue by filing timely objections to this Opinion . . . ."); *Smith*, 296 F. Supp. 2d 747, 765 (S.D. Tex. 2005) ("[This opinion] is written in the full expectation and hope that the government will seek appropriate review by higher courts so that guidance will be given the magistrate judges who are called upon to rule on these applications on a daily basis.").

C. The NSA Cases

> Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[209]

Justice Brandeis, dissenting in *Olmstead v. United States*, presciently wrote of a state of affairs that, as a practical matter, exists today. The following cases illustrate the legal challenges created by modern surveillance technology.

1. *ACLU v. NSA*

On December 19, 2005, President Bush acknowledged at a national press conference that the government had secretly started and continued to operate a massive electronic surveillance program. Rumors of the program had surfaced several days earlier in an article in *The New York Times* and other national newspapers.[210] President Bush asserted that the secret program was legal: "[C]onsistent with U.S. law and the Constitution, I authorized the interception of international communications of people with known links to al Qaeda and related terrorist organizations."[211] He also noted that "these calls are not intercepted within the country," and explained that the program only covered international calls, not domestic calls.[212]

A number of recent lawsuits have sought injunctions prohibiting the National Security Agency ("NSA") and other governmental entities from obtaining access to information through covert electronic surveillance programs conducted by the U.S. government.[213] In *ACLU v. NSA*, plaintiffs alleged that the Terrorist Surveillance Program ("TSP") intercepted the international electronic communications

---

[209] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

[210] *See, e.g.*, Dan Eggen, *Bush Authorized Domestic Spying*, WASH. POST, Dec. 16, 2005, at A1; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec., 16, 2005 at A1.

[211] Bush, *supra* note 6.

[212] *Id.*

[213] ACLU v. NSA, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *rev'd & dismissed by* ACLU v. NSA, 493 F.3d 644, 688 (6th Cir. 2007), *cert. petition pending, docket number not currently available*; Hepting v. AT&T, 439 F. Supp. 2d 974, 978-80 (N.D. Cal. 2006). A number of similar cases from jurisdictions around the country have been consolidated in a Federal Multi-District Litigation pursuant to 28 U.S.C. § 1407. *In re* NSA Telecomms. Records Litig., 474 F. Supp. 2d 1355, 1356 (J.P.M.L. 2007); *In re* NSA Telecoms. Records Litig., 444 F. Supp. 2d 1332, 1335 (J.P.M.L. 2006).

between American citizens and persons or entities affiliated with al Qaeda.[214] Plaintiffs included a group of journalists and attorneys who engaged in international communications with entities suspected of having ties with al Qaeda. The complaint alleged the TSP violated: (1) free speech and freedom of association guaranteed by First Amendment; (2) the "right to privacy" guaranteed by the Fourth Amendment; (3) the constitutional separation of powers in that the executive usurped the lawful bounds of the authority granted to him by Congress; (4) statutory anti-wiretapping laws, including FISA, because there was no oversight to the surveillance program; and (5) the Administrative Procedures Act ("APA").[215]

In response to the lawsuit, the government asserted the state secrets privilege and requested dismissal of the action.[216] The plaintiffs then filed a motion for summary judgment. The government responded to the motion for summary judgment by first requesting a stay of the motion pending the court's decision on the government's assertion of the state secrets privilege.[217] The district court denied the request for a stay. The government then responded to the motion for summary judgment by again asserting the state secret privilege and by asserting that the plaintiffs lacked standing. Notably, the government did not respond to the merits of the allegations.

The court held that the state secrets privilege applied to those aspects of the TSP that had not been publicly disclosed, but declined to apply the privilege to aspects of the program that had been publicly disclosed by the President.[218] The district court granted in part and denied in part the ACLU's request for a temporary restraining order enjoining the NSA and other agents of the United States from intercepting the electronic communications.[219] Addressing the standing issue, the district court found that the plaintiffs had asserted specific injuries that entitled them to relief; accordingly, the court granted the plaintiffs' summary judgment motion.

The government appealed to the Sixth Circuit. Immediately preceding oral argument, the government publicly announced that the TSP had been abandoned and that the government had obtained warrants under FISA for its surveillance operations. At oral argument

---

[214] *ACLU*, 438 F. Supp. 2d at 758.

[215] *Id.* at 758-59.

[216] *Id.*

[217] *Id.* at 758-60.

[218] *Id.* at 782.

[219] *Id.*

on January 31, 2007, the government asserted that the suit should be dismissed as moot and that the plaintiffs lacked standing.[220]

On July 6, 2007, the Sixth Circuit, in a split decision, reversed the decision of the district court by finding that the plaintiffs had failed to meet the requirements for standing to assert their constitutional and statutory claims.[221] The court of appeals ordered the case remanded to the district court for dismissal.[222]

2. *Hepting v. AT&T*

In a similar case in the Northern District of California, *Hepting v. AT&T*,[223] plaintiffs alleged that the government, primarily through the NSA, had "instituted a comprehensive and warrantless electronic surveillance program that violates the Constitution and ignores the careful safeguards set forth by Congress."[224] According to the detailed

[220] The use of the standing doctrine to bar actions to enforce constitutional rights of the People against the executive branch presents a rich topic for future scholarly attention.

[221] ACLU v. NSA, 493 F.3d 644, 688 (6th Cir. 2007). The opinion itself reflects the fractured nature of the reasoning behind the court's decision on the standing issue. Under Judge Batchelder's view, the plaintiffs had no standing unless they could establish injuries that resulted directly from being "regulated, constrained, or compelled" by government action. *Id.* at 655-57. In Batchelder's view, plaintiffs would have to establish not only that they were personally subject to the surveillance, but also that they suffered concrete injuries as a direct result of the surveillance. *Id.* Judge Gibbons concurred in the result but the essence of her opinion focused on the plaintiffs' lack of proof that they were actually subject to electronic surveillance. The first footnote of Judge Gibbons's opinion summarizes the distinction between her own opinion and the position of Judge Batchelder. *Id.* at 688 (Gibbons, Cir. J., concurring) ("The disposition of all of plaintiff's claims depends upon the single fact that the plaintiffs have failed to provide evidence that they are personally subject to the TSP.") In dissent, Judge Gilman rejected both the standard for standing set forth by the concurring judges and the application of the standard to the claims asserted by the plaintiffs in *ACLU v. NSA*. *Id.* at 697 (Gilman, dissenting). Judge Gilman differed from both Judge Batchelder and Judge Gibbons in finding that the plaintiffs did not need to establish actual surveillance by the government in order to survive a standing challenge. *Id.* at 702. ("[T]he critical question in this case is not whether the attorney plaintiffs have actually been surveilled — because as the lead opinion aptly notes, a wiretap by its nature is meant to be unknown to its targets — but whether the 'reasonableness of the fear' of such surveillance is sufficient to establish that they have suffered actual, imminent, concrete, or particularized harm from the government's alleged unlawful action.").

[222] *ACLU*, 493 F.3d at 688.

[223] 439 F. Supp. 2d 974, 978 (N.D. Cal. 2006).

[224] First Amended Complaint at 3, Hepting v. AT&T, 439 F. Supp. 2d 974 (July 20, 2007) (No. C-06-672). *Hepting* included affidavits from engineering and computational experts, who described the capacity and reach of the NSA program

allegations in the complaint, the defendant telephone company, AT&T, "opened its key telecommunications facilities and databases to direct access by the NSA and/or other governmental agencies, intercepting and disclosing to the government the contents of its customers' communications as well as detailed communications records about millions of its customers."[225] Specifically, plaintiffs alleged AT&T allowed the government to install a device that split the signal carried on AT&T's Internet trunk lines.[226] Plaintiffs averred that by failing to obtain the proper judicial authorization for the electronic surveillance, AT&T and the government violated the First and Fourth Amendments to the Constitution, FISA, Title III, section 605 of the Communications Act, the Stored Communications Act, and the Pen Register Act.[227]

The government moved to intervene and asserted the state secrets privilege. The court denied the government's petition to dismiss the action, but thereafter requested that the parties determine whether aspects of the case should be stayed pending appellate review of the district court's decision on the state secrets privilege.[228] This case is currently pending in the Ninth Circuit Court of Appeals.[229]

3. The State Secrets Privilege

The outcome of the NSA cases should depend on the treatment of the state secrets privilege by the courts of appeal.[230] The government has traditionally asserted the state secrets privilege in cases where the very existence of the lawsuit will reveal sensitive information. In 1875, in *Totten v. United States*,[231] plaintiff initiated an action for breach of contract against the government for espionage services during the Civil War. Justice Stephen Field, writing for the Court, affirmed the dismissal of the case, noting the primacy of the need for

based on their observations and knowledge of the field. Essentially, they described a system that diverts Internet traffic at the AT&T switching stations (AT&T, as a Tier 1 Internet provider, does not connect to the Internet; it is the Internet) to a NSA installation where, allegedly, the packet information is searched at the content level and targeted for further investigation.

[225] *Id.* at 6.

[226] *Id.* at 42-47.

[227] *Id.* at 78-149.

[228] *Hepting*, 439 F. Supp. 2d at 1011.

[229] Hepting v. AT&T, Nos. 06-17132 & 06-17137, 2007 U.S. App. LEXIS 26569 (9th Cir. Nov. 16, 2007).

[230] *See infra* Part III.C.3.

[231] 92 U.S. 105, 105-06 (1875).

secrecy and that the publicity of this type of contract constituted a breach barring recovery.[232] In *Tenet v. Doe*,[233] the Court, in an opinion by Chief Justice William Rehnquist, denied relief to former Cold War spies who had sued for breach of contract. The Court held, as in *Totten*, that revealing the existence of the espionage contracts precluded the action.[234]

The government has asserted the state secrets privilege where it cannot disclose information critical either to the plaintiff's prima facie case or to the government's defense of a claim. If the discovery process would necessarily reveal state secrets, the action may be dismissed. In *Kasza v. Browner*, the plaintiff alleged that the activities at a secret military installation were causing environmental damage in violation of the Resource Conservation and Recovery Act.[235] Plaintiff could not establish one of the elements of its claim without an admission from the government, which asserted the state secrets privilege.[236] The Ninth Circuit affirmed the assertion of the privilege and the district court's dismissal because the plaintiff could not establish one of the elements of its claim without revealing the secret material.[237] Likewise, in *Reynolds v. United States*,[238] the Court denied a tort claim by widows of victims of a B-29 crash, holding that the details of the secret mission and crash report, which would have been disclosed in the discovery process, were state secrets.[239]

The government has also asserted the state secrets privilege in cases involving alleged violations of the Fourth Amendment through the government's illegal wiretapping and surveillance. In *Tenenbaum v. Simonini*, the plaintiffs sued the employees of various U.S. agencies for engaging in illegal espionage.[240] The plaintiffs also alleged the decision to target them for espionage activities was motivated by their religious affiliation.[241] The government responded that it could not properly present a defense to these claims without revealing state

[232] *Id.* at 107.
[233] 544 U.S. 1 (2005).
[234] *Id.* at 11.
[235] 133 F.3d 1159, 1162 (9th Cir. 1998).
[236] *Id.* at 1163.
[237] *Id.* at 1169.
[238] 345 U.S. 1 (1953).
[239] *Id.* at 10.
[240] 372 F.3d 776, 777 (6th Cir. 2004).
[241] *Id.*

secrets.[242] The Sixth Circuit affirmed the district court's dismissal of the case on the state secret privilege.[243]

The public disclosure of a state secret may limit the validity of the privilege. In *Halkin v. Helms*, the government invoked the state secrets privilege in an action by Vietnam War protesters against the NSA, DIA, FBI, CIA, and Secret Service for warrantless wiretapping and illegal surveillance.[244] The District of Columbia Court of Appeals held that the state secrets privilege extended not only to details of a secret wiretapping and surveillance program in Operation Minaret, where details had not been publicly disclosed, but also to details of wiretapping and surveillance under Operation Shamrock, where details of the program had already been disclosed in congressional hearings.[245] But in *Ellsberg v. Mitchell*,[246] the same court held that the state secrets privilege is "not to be lightly invoked," and that there is no reason to "suspend the general rule that the burden is on those seeking an exemption from the Fourth Amendment warrant requirement to show the need for it."[247]

Analysis of a state secrets claim should proceed along a three-part course. The first question is whether the privilege is asserted by a proper party. Because the privilege is not to be lightly asserted, the written claim must be made by the head of the agency and must aver that the impending litigation would compromise a government secret. The second level of analysis is whether the existence of the suit or the claim itself involves the disclosure of a state secret. In *Totten* and *Tenet*, for example, where the claim under adjudication was whether the government contracted for espionage services, the very existence of the claim would reveal a state secret. In this defined area, the assertion of the privilege will preclude judicial review of the claim; in effect, the court is divested of jurisdiction to hear the case.

If the court is satisfied that the litigation of the claim or the presentation of a defense to a claim would necessarily reveal state secrets, then the court must dismiss the claim. For example, in *Reynolds* and *Kasza*, the discovery process would have revealed state secrets related to the secret mission of the aircraft. In *Kasza*, the plaintiff could not establish a claim without an admission of the existence of a secret government program, and therefore the claim had

---

[242] *Id.*

[243] *Id.* at 778.

[244] 598 F.2d 1, 4 (D.C. Cir. 1978).

[245] *Id.* at 11; *see also* Halkin v. Helms, 690 F.2d 977, 989 n.49 (D.C. Cir. 1982).

[246] 709 F.2d 51 (D.C. Cir. 1983).

[247] *Id.* at 57, 68.

to be dismissed. Before granting the privilege, the court must determine whether the claimed secret is actually secret. Thus in *Helms v. Halkin*, the district court properly considered whether the details of Operation Shamrock had already been made public by the proper authorities. Finally, if the privilege is properly asserted, the court must determine whether the case can proceed without the evidence suppressed as a result of the exercise of the privilege.

4. Summary of the NSA Cases

The core of the analysis in both *ACLU* and *Hepting* lies in the interpretation of the state secrets privilege. Initially, both district courts found that the state secrets privilege could not be applied to the face of the lawsuit; the circumstances were clearly distinguishable from a case where the lawsuit itself would disclose some state secret, typically an espionage contract. Both district courts found that the existence of the TSP had been disclosed publicly, and therefore the state secrets privilege could not be used to prevent disclosure of the program itself. However, the Sixth Circuit dismissed *ACLU* for lack of standing by the plaintiff, so the state secrets issue will not be decided unless the Supreme Court grants certiorari.[248]

ACLU and *Hepting* force us to reconsider the state secrets privilege. If, as alleged in the NSA Cases, the government is undertaking a massive surveillance program that includes monitoring and searching the content of individual communications (in email or in digitized telephone conversations), the assertion of the state secrets privilege effectively insulates the government from the limitations of the Fourth Amendment. The traditional state secrets doctrine should be amended to incorporate an additional factor — that the interests of the parties potentially affected by the assertion of the state secrets privilege be weighed collectively against the national security interest. In the balancing test, constitutional interests deserve greater weight relative to other interests. Thus, in cases of espionage contracts, like *Totten* and *Tenet*, the collective interests of society would clearly outweigh the benefit to the single individual seeking performance of the contract. Likewise, in tort cases, such as *Reynolds*, the security interests of the nation clearly outweigh the interests of the individuals harmed by the plane crash. However, where the application of the state secrets doctrine would affect the constitutional rights of millions of Americans, the calculus should be different. In sum, the state

[248] A Supreme Court docket number has not yet been assigned to *ACLU*.

secrets privilege should not immunize the activities of the executive branch from review. Courts applying the state secrets privilege must balance the interests presented by the plaintiff against the interest of the government in preserving secrecy and national security.

The NSA Cases suggest an ominous reality, where the government has tapped into the Internet in order to surreptitiously record the electronic transactions of the People. The government has relied on either the state secrets privilege or on standing requirements to repel requests to divulge the extent of its activities. It is difficult to see how the Fourth Amendment, in its current condition, limits the authority of the executive branch or offers any protection to the People to keep the government from intruding into their lives, homes, papers, and effects.

III. RECLAIMING THE RIGHT OF THE PEOPLE TO BE SECURE

The *Katz* Court recognized that unchecked government surveillance impinged upon the right of the People to be secure. The decision appears to have been a genuine attempt to reconcile the Fourth Amendment with modern technological advances. In the cases leading up to *Katz*, the Court had rejected claims that government intrusions unrelated to specific property claims were covered by the Fourth Amendment. In shifting the focus of the Fourth Amendment from protection of places to protection of people, the *Katz* decision broke with past precedent.[249]

The problem with the *Katz* approach was not the shift to a protection of people rather than places, but rather the use of reasonable expectation of privacy as the standard to determine the application of the Fourth Amendment. The language of the reasonable expectation of privacy standard minimized the importance of the interest protected by the Fourth Amendment and invited later courts to equate the rights protected by the Fourth Amendment with absolute secrecy. The result has been a decrease, since *Katz*, in the degree of constitutional limitation on the activities of the executive branch. While Congress has enacted statutes to fill the gaps left by the absence of constitutional regulation, many of the statutes, particularly in recent years, advance the capability of the executive branch to intrude unchecked into the lives of the People.[250] The Pen Register Decisions and the NSA Cases highlight the continuing relevance of the

[249] Katz v. United States, 389 U.S. 347, 353 (1967).

[250] Professor Kerr recently argued that the legislature, rather than the courts are better suited to regulate electronic surveillance. Kerr, *supra* note 152, at 805. The full import of this issue deserves meaningful treatment in a separate article.

Fourth Amendment's original promise of protection to the People against the government. In this context we should consider a return to the original principles of the Fourth Amendment.

The Framers recognized the danger of unrestricted executive power. The English experience with the writs of assistance, as well as the colonists' own outrage at the abuses carried out under color of law, convinced the drafters of the Bill of Rights to include a prohibition against unreasonable searches and seizures in the form of the Fourth Amendment to the Constitution.[251] Thus, in order to protect the People from the government, the Constitution guaranteed to the People the right to be secure from unreasonable governmental intrusions and unrestrained executive authority.[252]

Recognizing the inevitable flow toward more advanced and more intrusive technologies, the *Katz* Court applied the promises of the Fourth Amendment to the modern reality of electronic surveillance. The *Katz* Court made two moves. The first move, in Justice Stewart's majority opinion, brought electronic surveillance under the umbrella of Fourth Amendment review by shifting the focus of the Fourth Amendment from places to people. The second move, in Justice Harlan's concurring opinion, created a test — the reasonable expectation of privacy — to analyze whether a specific type of intrusion rose to the level of a Fourth Amendment violation.

In this section I argue that Justice Harlan's move should be revisited. The reasonable expectation of privacy standard should be abandoned in favor of a test that reclaims the original language of the Fourth Amendment — the right to be secure. Removing the reasonable expectation of privacy from our Fourth Amendment discourse will resolve some of the confusion that has plagued jurisprudence in the post-*Katz* era. Where language fails to describe a particular interest — in this case the Fourth Amendment's right to be secure — we should expect the interest to become distorted, to commingle with other interests, and to erode the original meaning of the interest. The reasonable expectation of privacy standard does not adequately describe the protection of the right to be secure: the word "reasonable" creates a contingency resting on a normative acceptance or rejection of the expectation; the word "expectation" implies a less significant interest than the word "right"; and the word "privacy" does not capture the full extent of the protection afforded by being secure. By reclaiming the original language of the Constitution, we reinforce

[251] *See* U.S. CONST. amend. IV.

[252] *See id.*

the notion that the Fourth Amendment protects the People from the government. Further, by characterizing the Fourth Amendment's protection as a right rather than as a mere expectation, we reaffirm the important role that courts must play in our system of intragovernmental checks and balances.[253]

By redefining the protection of the Fourth Amendment as a security interest rather than a privacy interest, we dispel the false dichotomy between privacy and security. A definition of the interests protected by the right to be secure should focus on personal security rather than mere personal privacy. Reverting to the original language of the Constitution will expose the reality (known well to the Framers) that personal security can be threatened by domestic as well as foreign governments. Ultimately, a robust enforcement of the Fourth Amendment will increase, rather than decrease, the security of the People and of the nation.

A. Beyond the Reasonable Expectation of Privacy

A clean break from the reasonable expectation of privacy standard will generate clarity by (1) reducing the blurring effect of a reliance on a normative standard, (2) adopting a conception of Fourth Amendment protection from governmental intrusion that comports with the realities of modern technology, and (3) linguistically separating the different notions of privacy in our current legal lexicon.

First, the elimination of the reasonable expectation of privacy standard will reduce the instability created by reliance on a fluctuating normative standard. Under the *Katz* standard, the Fourth Amendment applies only where the expectation of privacy is both subjectively and objectively reasonable.[254] The level of Fourth Amendment protection necessarily changes according to factors related to the reasonableness of the expectation.[255] In addition, the reasonableness of a search or the use of a given technology turns upon whether the search is routinely performed or the technology widely distributed. For example, the Court in *Kyllo v. United States* suggested that the reasonableness of the government's use of a surveillance technology would depend on the general availability of the technology.[256] The threat, then, is that as

---

[253] *See* Ku, *supra* note 5, at 1337.

[254] *Katz*, 389 U.S. at 361.

[255] Smith v. Maryland, 442 U.S. 735, 740-41 (1979).

[256] Kyllo v. United States, 533 U.S. 27, 39 & n.6 ("The dissent argues that we have injected potential uncertainty into the Constitutional analysis by noting that whether or not the technology is in general public use would be a factor."); *see also id.* at 43

more robust technologies move into general usage, the protections of the Fourth Amendment dissipate.[257]

Second, a shift away from notions of privacy in the Fourth Amendment context will remedy the jurisprudential tendency to equate Fourth Amendment privacy interests with complete secrecy.[258] Since *Katz*, courts have held that there is no reasonable expectation of privacy, and therefore no Fourth Amendment protection, where the information in question could be observed from a public vantage point or when such information has been shared with another person or entity.[259] For example, the Court has held that there was no reasonable expectation of privacy in open fields or in movements on public highways because the areas were visible from a public vantage point.[260] Likewise, the Court found no reasonable expectation of privacy in bank records or telephone numbers dialed because the information had been shared with the bank and telephone company.[261] Thus, in the post-*Katz* world, the Fourth Amendment functionally offers protection only if there has been no exposure to the outside world.

The technological reality of the modern world is that almost every aspect of daily life is linked by electronic communications networks that fall outside of constitutional protection. The reasonable expectation of privacy standard, as refined by courts after the *Katz* decision, eviscerates the Fourth Amendment by placing virtually all aspects of one's personal life outside the areas protected by the Fourth Amendment, thereby insulating governmental intrusion and surveillance from constitutional review. Eliminating the reasonable expectation of privacy test and restoring the right to be secure would reinvigorate the Fourth Amendment's capacity to limit improper governmental intrusion.

(Stevens, J., dissenting).

[257] *Smith*, 442 U.S. at 741.

[258] *See* Colb, *supra* note 85, at 153-61.

[259] *See supra* Part II.A.

[260] Minnesota v. Carter, 525 U.S. 83, 85 (1998) (holding no standing to claim reasonable expectation of privacy in activities inside home that were observed through gap in closed blind); Oliver v. United States, 466 U.S. 170, 177 (1984), (holding no reasonable expectation of privacy in barn surrounded by fenced land posted with no trespassing signs); United States v. Knotts, 460 U.S. 276, 282 (1983) (holding no reasonable expectation of privacy in location of public highways).

[261] *Smith*, 442 U.S. at 741 (holding no reasonable expectation of privacy in dialing information transmitted to telephone company); Miller v. United States, 425 U.S. 435, 442-44 (1976) (holding financial information shared with bank has no reasonable expectation of privacy).

Third, the removal of privacy language in the Fourth Amendment context will clarify the meaning of privacy in other legal contexts. In our current framework, privacy describes two types of legal interests. One privacy interest relates to personal choices, such as procreation or contraception, which are protected by the Fifth and Fourteenth Amendments.[262] The Fourth Amendment jurisprudence refers to a different privacy interest.[263] One commentator, Professor Sherry Colb, distinguished substantive privacy issues, such as contraception and procreation, from the Fourth Amendment's procedural privacy issues.[264] Professor Colb noted that government intrusions in the area of substantive privacy rights must meet a "narrow tailoring to a compelling interest" standard.[265] While the distinction between different types of privacy interests is helpful, and indeed critical to a meaningful analysis of privacy in our current legal framework, the separation of the Fourth Amendment's reasonable expectation of privacy from the discourse surrounding substantive privacy will eliminate confusion and confine our legal concept of privacy to substantive privacy issues.[266]

Once the reasonable expectation of privacy language is removed from our Fourth Amendment discourse, we can rely on the original language and intent of the Constitution to provide useful language to describe and fortify the interest protected by the Fourth Amendment. By reclaiming the original language of the Fourth Amendment, courts

---

[262] *See* Roe v. Wade, 410 U.S. 113 (1973) (finding constitutional right to privacy is broad enough to encompass decision to have children); Griswold v. Connecticut, 381 U.S. 479 (1965) (holding that Connecticut law forbidding use of contraceptives unconstitutionally intrudes upon right of marital privacy).

[263] With a single word change, we could have had a "reasonable expectation of *security*," defined by the subjective and objective standards described in Justice Harlan's concurrence. Justice Black might have found it more difficult to respond to the majority and concurring opinions in *Katz* if the word "security" had been substituted for the word "privacy." Katz v. United States, 389 U.S. 347, 360-62 (1967) (Harlan, J., concurring); *id.* at 364 (Black, J., dissenting).

[264] Sherry Colb, *The Qualitative Dimensions of the Fourth Amendment's "Reasonableness*," 98 COLUM. L. REV. 1642, 1643 (1998) (arguing protected interest is liberty to engage in particular activities or to enjoy certain status).

[265] *Id.* at 1642-46 (recognizing requirement that government intrusions meet "narrow tailoring to a compelling interest" standard in substantive privacy rights, and suggesting that reasonableness determinations in Fourth Amendment searches be determined by weighing government's interest in conducting search against individual's interest in remaining free from governmental intrusion).

[266] It may well be that the right to security guaranteed by the Fourth Amendment could be analyzed with the same metric used in substantive privacy claims — a narrow tailoring of government interests to meet a compelling state interest — however, I will reserve that issue for future discussion.

can revive the original purpose of the Amendment as a limitation on governmental authority.

B. Defining the Right to be Secure

The Framers of the Constitution guaranteed to the People the right to be secure in their persons, papers, houses, and effects.[267] The right to be secure, however, has defied precise definition despite the well-intentioned efforts of courts and commentators. Some of the Court's decisions speak of the right to be secure in terms of the sanctity of the home.[268] Before *Katz*, several dissenting opinions expressed the view that the Fourth Amendment protected a generalized right to be let alone.[269] The most famous of these, of course, was Justice Brandeis's opinion in *Olmstead*, where he stated: "The makers of our Constitution . . . conferred, as against the government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men."[270] Other Justices agreed with the view expressed by Justice Brandeis. For example, the dissenting opinions of Justice Douglas and Justice Burton in *On Lee v. United States* supported a view of the Fourth Amendment as protecting the right to be let alone.[271] Further, in *Hoffa v. United States*, the Court stated that "[the Fourth Amendment protects] the security a man relies upon when he places himself or his property within a constitutionally protected area . . . ."[272]

One commentator has suggested that the Fourth Amendment should be understood as a right to exclude.[273] The conception of the right to be secure as a right to exclude is alluring because it explains both the historic relationship between the Fourth Amendment and property rights and the modern need to protect the People against governmental intrusions that are not based in physical trespass. The

---

[267] *See* U.S. CONST. amend IV.

[268] *See, e.g.*, Silverman v. United States, 365 U.S. 505, 511 (1961) ("At the very core stands the right of a man to retreat into his own home . . . ."); *see also* Payton v. New York, 445 U.S. 573, 586 (1980).

[269] *See, e.g.*, *Silverman*, 365 U.S. at 511.

[270] Olmstead v. United States, 277 U.S. 438, 478-79 (1928) (Brandeis, J., dissenting).

[271] *See* On Lee v. United States, 343 U.S. 747, 762-65 (1952) (Douglas, J., dissenting); *id.* at 765-67 (Burton, J., dissenting); *Olmstead*, 277 U.S. at 478-79; *cf.* Katz v. United States, 389 U.S. 347, 350 (1967) (Black, J., dissenting).

[272] 385 U.S. 293, 301 (1966).

[273] Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 354-56 (1998).

right to be secure should include a right to exclude, but standing alone, a right to exclude is insufficient to protect the entire scope of interests covered by the Amendment's right to be secure. Another commentator, Professor Ray Ku, argued that the Fourth Amendment is concerned with power, not privacy, and should be viewed as a mechanism for enforcing the separation and limitation of governmental powers.[274]

A broader reading of the interests involved in the right to be secure would cast the right as an amalgam of several constitutional protections. In this expanded reading, the Constitution created a general right protecting the People from governmental interference. The right of the people to be secure includes the freedom to associate with individuals or groups, freedom of expressions of belief, freedom of movement, freedom to create and present ideas, as well as the negative expressions of these freedoms.[275] In many contexts, the practical expressions of constitutional values are dependent upon the capacity of the People to control the flow of information about their own identity.

C. The Role of the Courts

The courts must be more proactive in their role in limiting the reach of the executive branch. Both the Pen Register Decisions and the NSA Cases presented Fourth Amendment issues in a context that suggest a greater role for the courts. In the traditional conception of the adversarial system, the court plays the role of neutral arbiter, deciding only the issues framed by the parties, based on the evidence provided by the parties. [276] However, in the constitutional context, and particularly in the context of ex parte proceedings, the courts must protect the unrepresented interests of the People. Courts should assume the additional obligation of assuring that the government does not reach further than permitted by the Fourth Amendment and the relevant statutory structure. If courts are not comfortable accepting this role, and many may not be, then they should freely explore alternative measures to ensure the representation of the interests of the People. The Pen Register Decisions suggest one immediate

[274] Ku, *supra* note 5, at 1326 ("The Fourth Amendment protects power, not privacy.").

[275] *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (arguing for recognition of general right to privacy).

[276] *See* Abram Chayes, *The Role of the Judge in Public Law Litigation*, 89 HARV. L. REV. 1281, 1283-84 (1976) (describing traditional role of court as neutral arbiter).

remedial measure.[277] Commendably, a few courts appointed amici to brief the position opposed to the government.[278] The appointment of counsel to represent the interests of the People would identify the separate interests of the collective people and would encourage a more thorough litigation of the issues before the courts.

From an institutional perspective, courts must accept their role of enforcing the Constitution against the executive branch by applying greater scrutiny to executive claims of authority. The NSA Cases present the courts with an opportunity to revisit the difficult issue of the state secrets privilege. As discussed earlier, the application of the state secrets privilege should be subject to a balancing test where the significance of the interests at stake in the lawsuit are fairly weighed in the determination of whether the privilege applies. The privilege itself rests on the proposition that some interests, such as national security, are superior to other types of interests, such as the individual claims in a lawsuit. However, where the interest asserted in the lawsuit is not a claim for breach of contract but a claim for breach of the Constitution, the application of the privilege should not be taken lightly.

The difficulty in apportioning proper weight to the interests protected by the Fourth Amendment stems from the use of the language in the reasonable expectation of privacy test. Reclaiming the language of the Fourth Amendment implies a different role for the courts because the original language denotes a right, rather than an expectation. An expression of the interests protected by the Fourth Amendment as a right rather than as an expectation necessarily entails a higher degree of involvement for the courts. If we expect to restore significance to the promise of the Fourth Amendment, we must encourage courts to abandon the reasonable expectation of privacy test. We cannot reasonably expect the executive branch to limit itself, nor can we expect the legislative branch to successfully restrain the executive. The Constitution's original promise to the People of a right to be secure cannot survive without a renewed commitment and vigilance from the courts.

---

[277] Recall that the Pen Register Decisions involved ex parte applications for orders that provided the government with location information on subject telephones without a warrant and without suspicion of criminal conduct. Further, the owner of the subject telephone would have no knowledge of the monitoring. Unless the government sought to introduce evidence from the monitoring at a criminal trial of the owner, there would be no opportunity to challenge the actions of the government.

[278] *Gorenstein*, 405 F. Supp. 2d 435, 436 (S.D.N.Y. 2005) (asking Federal Defender to appear as amici); *see Orenstein II*, 396 F. Supp. 2d 294, 295 (E.D.N.Y. 2005) (noting Electronic Frontier Foundation appeared as amici).

CONCLUSION

As we pause to reflect on the fortieth anniversary of the Supreme Court's decision in *Katz v. United States*, we would do well to reconsider the modern contours of a reasonable expectation of privacy, and whether, owing to the pervasive capability of modern technology to easily intrude into the most intimate details of our life, the People have any expectation of privacy or right to be secure. Much of the discussion in recent years has focused on the need for security, with an implication that the interests represented by security are at odds with the interests represented by privacy.

Recent cases demonstrate that our Fourth Amendment jurisprudence is on the verge of collapse and will only survive if courts reclaim the original meaning and language of the Constitution. The next paradigm shift must include a departure from *Katz*'s use of privacy language, and focus instead on the right of the People to be secure. Fundamental to the modern conception of personal security, and indeed one of the basic precepts of the Founding Fathers, is the idea that the government does not ensure the security of the People, but rather that the government embodies the interest against which the People must be protected. Reclaiming the original language of the Constitution by substituting a right to personal security for a reasonable expectation of privacy will simultaneously dispel the false notion that the Fourth Amendment protects individual interests in opposition to collective interests, and reaffirm the idea that only by protecting individual security will we increase our collective personal and national security.